清華大學 计算机系列教材

王爱英 编著

物联网与智能卡技术基础



清华大学出版社

清华大学计算机系列教材

物联网与智能卡技术基础

王爱英　编著

清华大学出版社
北　京

内 容 简 介

物联网是在计算机、互联网和移动通信技术的基础上，采用智能卡、射频识别标签、传感器等设备组成的，设备与设备或网络之间，可通过固定导线或空中射频接口传送数据。

智能卡是射频识别(RFID)标签的前驱，在中国居民身份证、金融卡和手机 SIM 卡的发行量早已超过几十亿张，在技术、功能、安全和标准制定等方面可供 RFID 借鉴。

本书主要内容包括计算机和互联网的基础知识，射频信号的处理与频段分配，智能卡、RFID 标签和传感器的硬件结构，智能化设备的操作系统与测试，空中传输信号的防冲突方案，纠错、识别、安全和防欺诈措施、国际标准，以及互联网、物联网的应用和创新。

本书主要提供给高等院校的信息技术、计算机、通信、自动控制和物联网等专业作为技术基础课的教材。

图书在版编目(CIP)数据

物联网与智能卡技术基础/王爱英编著. —北京：清华大学出版社，2019
(清华大学计算机系列教材)
ISBN 978-7-302-49456-0

Ⅰ. ①物…　Ⅱ. ①王…　Ⅲ. ①互联网络－应用－高等学校－教材 ②IC 卡－技术－高等学校－教材　Ⅳ. ①TP393.4 ②TN43

中国版本图书馆 CIP 数据核字(2018)第 020925 号

责任编辑：白立军　王冰飞
封面设计：常雪影
责任校对：时翠兰
责任印制：宋　林

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦 A 座　　**邮　　编：**100084
社 总 机：010-62770175　　**邮　　购：**010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课件下载：http://www.tup.com.cn，010-62795954
印 刷 者：北京富博印刷有限公司
装 订 者：北京市密云县京文制本装订厂
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张：**17　　**字　　数：**389 千字
版　　次：2019 年 1 月第 1 版　　**印　　次：**2019 年 1 月第1 次印刷
定　　价：45.00 元

产品编号：076472-01

序

“清华大学计算机系列教材”已经出版发行了30余种，包括计算机科学与技术专业的基础数学、专业技术基础和专业等课程的教材，覆盖了计算机科学与技术专业本科生和研究生的主要教学内容。这是一批至今发行数量很大并赢得广大读者赞誉的书籍，是近年来出版的大学计算机专业教材中影响比较大的一批精品。

本系列教材的作者都是我熟悉的教授与同事，他们长期在第一线担任相关课程的教学工作，是一批很受本科生和研究生欢迎的任课教师。编写高质量的计算机专业本科生（和研究生）教材，不仅需要作者具备丰富的教学经验和科研实践，还需要对相关领域科技发展前沿的正确把握和了解。正因为本系列教材的作者具备了这些条件，才有了这批高质量优秀教材的产生。可以说，教材是他们长期辛勤工作的结晶。本系列教材出版发行以来，从其发行的数量、读者的反映、已经获得的国家级与省部级的奖励，以及在各个高等院校教学中所发挥的作用上，都可以看出本系列教材所产生的社会影响与效益。

计算机学科发展异常迅速，内容更新很快。作为教材，一方面要反映本领域基础性、普遍性的知识，保持内容的相对稳定性；另一方面，又需要跟踪科技的发展，及时地调整和更新内容。本系列教材都能按照自身的需要及时地做到这一点。例如，王爱英教授等编著的《计算机组成与结构（第5版）》、戴梅萼教授等编著的《微型计算机技术及应用（第四版）》都已经出版了，严蔚敏教授的《数据结构》也出版了第三版，使教材既保持了稳定性，又达到了先进性的要求。

本系列教材内容丰富，体系结构严谨，概念清晰，易学易懂，符合学生的认知规律，适合于教学与自学，深受广大读者的欢迎。系列教材中多数配有丰富的习题集、习题解答、上机及实验指导和电子教案，便于学生理论联系实际地学习相关课程。

随着我国进一步的开放，我们需要扩大国际交流，加强学习国外的先进经验。在大学教材建设上，我们也应该注意学习和引进国外的先进教材。但是，“清华大学计算机系列教材”的出版发行实践及它所取得的效果告诉我们，在当前形势下，编写符合国情的具有自主版权的高质量教材仍具有重大意义和价值。它与国外原版教材不仅不矛盾，而且是相辅相成的。本系列教材的出版还表明，针对某一学科培养的要求，在教育部等上级部门的指导下，有计划地组织任课教师编写系列教材，还促进了对该学科科学、合理的教学体系和内容的研究。

我希望今后有更多、更好的优秀教材出版。

清华大学计算机系教授，中国科学院院士

张钹

前　　言

集成电路、计算机、互联网和移动通信技术的应用,促进了物联网的诞生与发展。计算机的使用改变了人类传统的计算方法和对万物的控制能力,智能化的理念已普及各个领域,计算机或微处理器的应用已深入军事、经济、商务、工业控制、通信、文化、游戏、影视等各个方面。

智能手机、平板电脑已成为可随身携带的电话机、计算机。

智能卡的发行量在我国已超过几十亿张,无论是在应用、安全还是在一卡多用等方面都有扩展,性能在提高而产品的价格在下降。物联网的应用向射频识别(RFID)和传感器等产品在技术、性能和质量等方面提出了要求。在人工智能方面,语音识别、机器翻译、人机对话、机器人、无人驾驶飞机和汽车等领域已取得进展。

物联网、互联网、移动通信网的功能相互渗透。平板电脑、智能手机的科技水平和服务内容竞争激烈并趋向一致。大屏幕的智能电视机虽然不能移动,但发展前景毋庸置疑。

我国在军事、经济、科技和工业等领域都向国际水平追赶、迈进,在某些方面已处于举足轻重或领先地位,因此人才的培养极为重要。我国已有几十所大学增设了物联网专业。

自 20 世纪 90 年代开始,清华大学和中国电子技术标准化研究院,联合相应的智能卡研发公司,完成智能卡的设计、制造和标准制定工作,为教学与应用付出了劳动。中国电子技术标准化研究院与社会各界联合提出的标准经上级批准后,发布为国家标准,并申请了专利。

1996 年,参加 IC 卡研发的清华大学教授和研究生编写了《智能卡技术》一书。20 世纪 90 年代正值 IC 卡在国内兴起之时,该书成为不少业界人士的参考书或入门培训教材。随着科技和应用的发展和创新,2015 年《智能卡技术(第四版)——IC 卡、RFID 标签与物联网》问世,并萌发了编写物联网与智能卡技术基础教材的设想。

2016 年,电子技术标准化研究院的金倩和冯敬两位高级工程师为本书的编写提供了资料。

本书是为高等院校培养物联网与相关领域的“产、学、研、用”人才而编写的技术基础教材,为后续的学习和工作服务做准备。当今技术飞速发展,学习不能间断,对作者来说也是这样,书中的某些内容会很快地被新技术更新,但不会很快地被排斥。书中难免存在疏漏和不妥之处,欢迎广大读者指正。

作者

2018 年 5 月

目　录

第 1 章　概　　论

在全球范围内，无论是军事领域还是民用领域，集成电路、计算机、互联网和移动通信技术都得到蓬勃的发展和广泛的应用，从而促进了智能标识（智能卡、射频识别标签等）和物联网的产生、发展和应用。

在中国，智能卡广泛应用于居民身份证、金融卡、手机中的 SIM 卡、交通卡、移动终端和门禁系统等方面，已发行几十亿张，并从有线技术向无线技术方向发展，促进了互联网、物联网和移动通信网的融合。

智能卡和射频识别标签用于识别“人”和“物”，并根据应用需求完成其与读写器之间的数据传送、数据处理等。

物联网是指通过各种信息传感设备，如传感器、射频识别标签和 IC 卡等，实时采集各个物品需要监控的信息，并进行处理，是实现人与人、物与物、人与物连接的网络。

1.1　计算机的应用

计算机是从军事上的科研和应用开始的，并推广到下述各方面。

1. 科学计算

在国防、尖端科学技术、数学等学科领域要进行大量的复杂运算，具有计算量大、数据值变化范围大等特点。高性能计算机在先进集成电路工艺的支持下，具有浮点运算和信号处理等功能。

2. 数据处理

在金融企业与管理等领域内，数据处理具有大量数据输入、存储和处理功能，其主要特点是运算比较简单、联系比较广泛（个人、单位、银行、政府、国际），要求精确、安全、防诈骗。

当前在数据中心、大数据和云服务领域有很大发展。

3. 计算机控制

在工业生产和交通运输等过程中的自动控制，包括零部件的设计与制造（传感器、仪器、设备等）和整机组装。

4. 人工智能

人工智能包括知识获取与处理、语音识别、图像处理、搜索、下棋、智能机器人。

其他方面的应用不胜枚举，近年来发展极为迅速，计算机和互联网的发展和应用已普及（参见 2.2 节），并深入到各个领域，在大学中有很多专业将它列为必学的基础课程。

1.2　智能卡、射频识别标签与读写器

1. 智能卡与读写器

智能卡（Smart Card）又称集成电路卡，即 IC 卡（Integrated Circuit card）。它将一个

集成电路芯片镶嵌于塑料基片中，封装成卡的形式，其外形与覆盖磁条的磁卡相似。

IC 卡的概念是 20 世纪 70 年代初提出来的，它将微电子技术和计算机技术结合在一起，提高了人们生活和工作的现代化程度。

IC 卡芯片具有写入数据、存储数据和读出数据的能力，IC 卡存储器中的内容根据需要可以有条件地供外部读取，或者供内部信息处理和判定之用。根据卡中所镶嵌的集成电路的不同，IC 卡可以分为以下两类。

(1) 逻辑加密卡。卡中的集成电路具有加密逻辑功能和 E^2PROM(可用电擦除的可编程只读存储器)。

(2) 智能卡(CPU 卡)。卡中的集成电路包括微处理器、E^2PROM、随机存储器(Random Access Memory，RAM)，以及固化在只读存储器(Read Only Memory，ROM)中的片内操作系统(Chip Operating System，COS)。随着集成电路工艺的提高、价格的下降，当前主要使用智能卡。

按应用领域来分，IC 卡分为金融卡和非金融卡两种。金融卡又分为信用卡(credit card)和现金卡(debit card)等。信用卡主要由银行发行和管理，持卡人用它作为消费时的支付工具，可以使用预先设定的透支限额资金；现金卡又称储蓄卡，可用作电子存折和电子钱包，不允许透支。非金融卡往往出现在各种事务管理、安全管理场所，如身份证明、健康记录和职工考勤等。此外，还有一些预付费卡，如用于公交系统中的交通卡、超市中使用的购物卡等，由相应的管理单位发行。

按卡与外界数据传送的形式来分，有接触式 IC 卡和非接触式 IC 卡两种。在接触式 IC 卡上，IC 芯片有 8 个触点可与外界接触。非接触式 IC 卡的集成电路不向外引出触点，因此它除了包含前述 IC 卡的电路外，还带有射频收发电路、天线及其相关电路。非接触式卡出现较晚，但由于它具有一些接触式 IC 卡所不能替代的优点，因此在某些应用领域发展较快。

在 IC 卡推出之前，磁卡已得到广泛应用，为了从磁卡平稳过渡到 IC 卡，也是为了兼容，使某些 IC 卡仍保留磁卡原有的功能。也就是说，在 IC 卡上仍贴有磁条，因此 IC 卡也可同时作为磁卡使用。图 1.1 所示为兼有接触式和非接触式功能的 IC 卡外观示意图，正面中左侧的小方块中有 8 个触点，如果是金融卡，则其下面为凸形字符(账号)，背面有磁条。正面还可印刷各种图案，如身份证的人像。卡的尺寸、触点的位置与用途、磁条的位置及数据格式等均有相应的国际标准予以明确规定，卡内四周有天线。

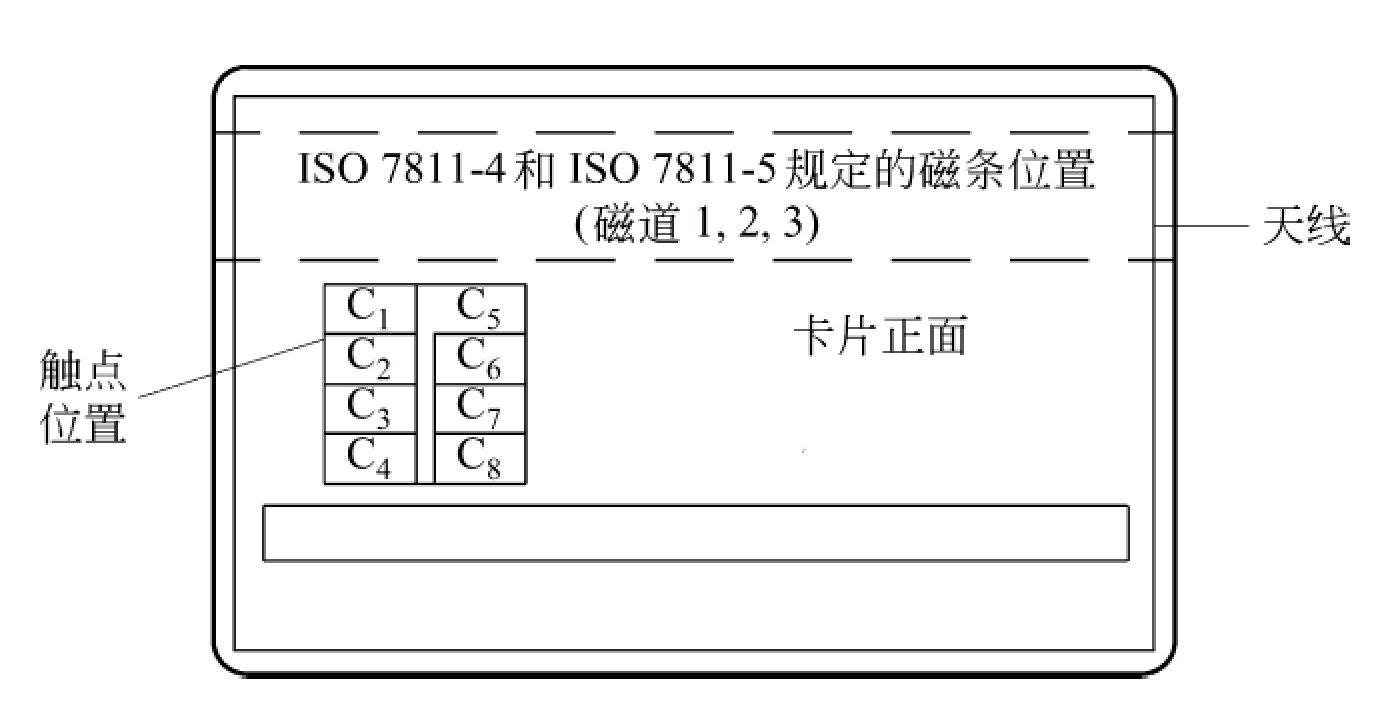


图 1.1 IC 卡的外观示意图

卡上有发行单位和持卡人的识别标志，可以称为“识别卡”。

2. IC 卡的读写器

为了使用卡片，还需要有与 IC 卡配合工作的读写器或称为接口设备（InterFace Device，IFD），IFD 是 interface device 的缩写词，从原词中选取字母，并用大写英文字母替代。IFD 可以是一个由微处理器、键盘、显示器与 I/O 接口组成的独立设备，通过 IC 卡上的 8 个触点或天线（射频电路）向 IC 卡提供电源，并与 IC 卡相互交换信息，也可以是一个简单的接口电路，IC 卡通过该电路与通用微机相连接。在卡上能存储的信息总是有限的，因此大部分信息需要存放在读写器或计算机中。

3. 射频识别标签与读写器

射频识别（Radio Frequency IDentification，RFID）技术的基本原理是利用无线射频信号的空间耦合（电磁感应或电磁传播）实现对被识别物体的自动识别。RFID 系统的基本工作方式是将 RFID 标签安装在被识别物体上（粘贴、嵌入、佩挂或植入等），当被识别物体进入 RFID 读写器的读写范围内（射频场）时，标签与读写器之间建立起联系，其过程一般由读写器启动，然后标签向读写器发送自身信息，如标签编号和标签内存储的数据等，读写器接收信息并解码后，传送给计算机进行处理。RFID 系统一般由两部分组成，即 RFID 和读写器，RFID 又称电子标签。电子标签和读写器内部都装有天线，电子标签所需的能量可从读写器的射频场内取得（无源标签）或自带电源（有源标签）。

非接触 IC 卡可认为是电子标签的一种。电子标签的形式多样化，且不引出触点。

由于在读写器的射频场内可能存在多张非接触式 IC 卡或 RFID 标签，因此读写双方都要增加功能，以实现读写器逐一联系标签的方法。

1.3 安全问题

智能卡可用作金融卡和非金融卡，其中金融卡需要处理的内容较多，并需重视安全问题。其主要功能是识别卡、读写器和持卡人的真假，以及存储数据和处理数据等。

1. 举例

下面以自动柜员机（Automatic Teller Machine，ATM）为例来说明金融卡取款操作过程。

自动柜员机是放在银行或商店大堂中供客户自动提款的机器(有的 ATM 还有自动存款功能)。执行从 ATM 提取现金的操作仅需十几秒钟，总共需要持卡人做出如下 4 个动作。

（1）插入金融卡，然后按 ATM 屏幕提示进行操作。

（2）输入个人标识码（Personal Identification Number，PIN），即输入密码。

（3）选择交易类型（取款）。

（4）给出申请提取的金额。

当 ATM 判别没有问题时，自动输出卡和现金，并打印凭证。ATM 是一种操作方便的信息处理系统，可以 24h 提供服务。假如存在任何问题，则在 ATM 的屏幕上显示存在的问题和下一步应该进行的操作。

ATM 是安装在柜里的计算机系统。它的内部有严密可靠的物理和逻辑安全措施。

它的每一笔交易通常接受正确的授权和严格的控制，因此ATM系统既是一个操作简单的系统，又是一个构造复杂的系统。

ATM将IC卡或磁条上(对磁卡)的数据，诸如发卡单位和客户账号识别码(用来获取自动授权信息的基础)通过通信线路与发卡单位的计算机及其账户数据库相连，用以检查金融卡的编号(查对黑名单)，以防止他人使用已挂失的或偷窃来的金融卡，同时核对客户的账面记录，以查明可供支用的金额，并根据交易的金额随即更新账面记录，供金融卡下次使用。此外，为了避免某些可能发生的弊端(如已挂失但尚未列入黑名单)，还要限制金融卡在一天内允许使用的次数和一天内允许提取现金的总金额。

绝大多数ATM取款时还需输入个人标识码PIN(即密码)，并将PIN传送到计算机，用来核对持卡人是否是卡的主人。例如，在通信线路上明文传送PIN，存在被窃听的危险，为此有时需对PIN进行加密，这就要提供一个加密算法和“密钥”，让经过加密后的PIN在通信线路上传送，在接收端解密，因此在接收端提出了密钥的管理和保护的要求。

2. 影响安全的若干基本问题

(1) 智能卡和读写器之间的信息流通。这些流通的信息可以被截取分析，从而可被复制或插入假信号。

(2) 模拟的智能卡(或伪造的智能卡)。模拟智能卡与读写器之间的信息，使读写器无法判断出是合法的还是模拟的智能卡。

(3) 非法使用他人的IC卡。因此要验证持卡人的身份。

(4) 诈骗。通过电信、电话等进行诈骗，骗取钱财。

(5) 篡改读写器的作弊行为。造成读/写卡中的数据不正确，因此不允许借用、私自拆卸或改装读写器。

其他卡有相似的或不同的安全问题(根据应用要求)。

3. 安全措施

为了安全防护，一般采取以下措施。

(1) 使用时，对持卡人、卡、标签和读写器的合法性要相互检验。

(2) 重要数据加密后传送。

(3) 检验数据的完整性，以防止卡内数据被删除、增加或修改，并纠正读写或传送时产生的差错。

(4) 设备中设置安全区，在安全区中包含有逻辑电路或外部不可读的存储区。如果有不合规范的操作，将自动禁止进一步操作。

(5) 设计、生产和发行的有关人员明确各自的责任，并严格遵守。相应的单位要取得合法认证。

(6) 设置黑名单。

(7) 对犯法行为进行法律制裁。

4. 密钥与认证

1) 密钥

密钥是存放在卡和读写器中的秘密数码，绝对不允许向外界泄露，智能卡和读写器的相互认证及重要数据的发送和接收都是通过密钥和相应的密码算法实现的。在数据发送

方，用密钥对数据进行加密运算后发送；在接收方，用密钥对数据进行解密运算后恢复成加密前的数据。

与加密和解密有关的还有密钥管理。密钥管理包括密钥的生成、分配、保管和销毁等。

对传输的信息进行加密，以防被窃取、更改，从而避免造成损失。对存储的信息进行加密保护，使得只有掌握密钥的人才能理解信息。

2）认证

（1）单位的合法性认证。对发行和运营等单位的合法性通过公正的权威机构进行认证。

（2）数字签名（电子签名）。要求：收方能确认发方的签名；发方签名后，不能否认自己的签名；发生矛盾时，公证人（第三方）能仲裁收、发方的问题。

（3）身份认证。用 password 或个人标识码 PIN 进行认证，或利用生物特征（指纹、人脸识别）进行认证。

密钥与认证问题将在第 5 章详细讨论。

1.4 国际标准

就标准而言，可以有国际标准、国家标准、行业标准和事实上的标准（工业标准）。其中，国际标准是由世界上一些国家或团体组成的国际标准化机构成员通过投票而确定的。在世界各地有多个国际标准化机构，其中影响较大的有国际标准化组织（International Organization for Standardization，ISO）、国际电工委员会（International Electrotechnical Commission，IEC）和国际电信联盟（International Telecommunication Union，ITU）。

国家标准是由国内的相关单位讨论通过并报请标准主管部门批准而确定的。

对一些影响范围相对较小或尚不完全成熟而确有实际需要的规范，则被确定为行业标准，这也需要经过行业主管部门批准。

某些单位或公司制定的一些规范，虽然没有经过有关标准化机构组织的讨论，但是由于其大量使用而造成不可忽视的影响，从而成为事实上的标准。

ISO 和 IEC 一起组成了国际标准化工作的专门委员会，作为 ISO 或 IEC 成员的国家团体通过技术委员会参与国际标准的制定。ISO 与 IEC 的技术委员会在彼此有兴趣的领域互相合作。

在信息技术领域，ISO 和 IEC 共同建立了一个技术委员会——ISO/IEC JTC 1，被该委员会所采纳的国际标准草案由各国家团体投票，被发布作为国际标准至少需要得到75％参加投票的国家团体的赞成。

已发布的国际标准，在今后仍可能被修改，因此，在使用国际标准时，要注意应用国际标准的最新版本。

我国在制定国家标准时，主要参照 ISO 的国际标准，因此在本书中主要讨论 ISO/IEC 制定的 IC 卡和 RFID 标签的国际标准。

1. IC 卡的国际标准

IC 卡分接触式 IC 卡和非接触式 IC 卡两种。接触式 IC 卡推广应用较早，而近年来

由于非接触式 IC 卡使用的便捷性及成本的下降，应用范围迅速扩大。

接触式 IC 卡遵循的是 ISO/IEC 7816 国际标准，非接触式 IC 卡国际标准为 ISO/IEC 14443 和 ISO/IEC 15693，以及 ISO/IEC 7816 中对非接触式 IC 卡也适用的部分标准。

(1) ISO/IEC 7816 国际标准的标题是识别卡—集成电路卡。

① 适用于接触式 IC 卡的部分有 7816-1/2/3/10/12。符号“/”解释为“或”，如 7816-1/2 表示为 7816-1 或 7816-2。

② 对接触式 IC 卡和非接触式 IC 卡均适用的部分有 7816-4/5/6/7/8/9/11/13/15。

(2) ISO/IEC 14443 国际标准的标题是识别卡—非接触式集成电路卡—接近式卡。

(3) ISO/IEC 15693 国际标准的标题是识别卡—非接触式集成电路卡—邻近式卡。

2. RFID 标签的国际标准

RFID 标签形状尺寸各异，应用范围极广，有多个国际标准化组织为之制定了国际标准。本书介绍了 ISO/IEC 18000 国际标准，该标准规定了空中接口协议。

根据标签与读写器之间的工作频率不同确定了 6 部分：ISO/IEC 18000-1/2/3/4/6/7。

此外，非接触 IC 卡的国际标准 ISO/IEC 15693 也适用于 RFID 标签。

3. 其他卡与标签使用的相关标准、规范、协议

(1) 互联网。

(2) 解决安全问题的密钥密码体制。

(3) 卡与标准中表示信息的数据元和数据对象。

在新的国际标准制定或有创新技术和产品出现时，一般都会申请相关的专利，应予以关注，以防经济上的纠纷。

1.5 物联网的诞生与发展

IC 卡、RFID 标签促进了物联网的诞生与发展。

1. 接触式 IC 卡

1977 年，Motorola 与它的一个计算机客户合作开发了一张智能卡，形成了第一代智能卡产品。该智能卡将一个可编程的微控制器及一个非易失性的存储器集成在一个模块内，然后嵌入到一张符合 ISO 7810 标准的信用卡中。该产品在法国进行了试验，目的是为了对进行脱机(off-line)交易所需的技术予以评估。自此以后，智能卡开始迅猛发展，它所采用的技术也日新月异地发生着变化。1979 年产生了世界上第一片专为智能卡所设计的单片机芯片，从而形成了第二代智能卡产品，并在法国、瑞士、斯堪的纳维亚得到应用。当时主要是用作银行卡(bank card)。进入 20 世纪 90 年代后，在通信、健康和交通等方面，智能卡的应用也开始蓬勃发展。

早期的智能卡大多是一种单功能卡，即一张卡只适用于某一种应用。以后的智能卡则向着多功能卡的方向发展。例如，可以发行城市卡(city card)，这种卡将包括用户在一个城市中可能经常需要接触的大部分应用功能，如作为电子钱包(electronic purses)、医

疗保健卡和交通卡使用等。后来智能卡与通信更为紧密地结合，在手机和网络管理等方面得到应用。

2. 非接触式 IC 卡和 RFID 标签

20 世纪 90 年代中期开始，产生了基于现代微电子技术和射频识别技术的多种非接触式 IC 卡。

在此之前，部分公司和半导体制造商已涉足射频技术产品的研发。RFID 技术最早的应用始于第二次世界大战期间的美国国防部军需供应局，用于识别在战争中本国和盟军的飞机，但由于昂贵的价格限制了其广泛应用。在美军对伊拉克的战争中，这一技术再次得到检验，在计算机软件系统的配合下，美军实现了对战略物资的准确调配。

1991 年，美国德州仪器（Texas Instrument，TI）公司专门成立一个分公司，致力于以 RFID 技术为基础的全球人员和物品信息的自动采集和识别方案的研究，不仅研发出适宜家畜管理和车辆防盗等用途的低频产品，而且推出了用于高速公路自动收费等的微波产品及人员和物资跟踪识别的高频电子标签等，为非标准式 IC 卡的研发和相关标准的制定提供了条件。

荷兰飞利浦半导体（Philips Semiconductors）公司是在非接触式 IC 卡发展历程中影响最大的公司，1992 年它的防冲突（anticollision）技术的发明和在 13.56MHz RFID 系统中的首次应用是对无源式 RFID 技术的重大突破。其产品所采用的技术成为后来制定的非接触 IC 卡国际标准 ISO/IEC 14443 Type A 的基础，并申请了多项专利。

与此同时，其他公司相继推出具有各自特点的产品，如 ST 半导体公司和以色列的 OTI 公司推出遵循 ISO/IEC 14443 Type B 国际标准的非接触式 IC 卡芯片。

拥有 2002 年全球 RFID 产品最大出货量的 EM 微电子公司，于 1990 年实现了只读式 RFID 芯片在信鸽比赛中的世界首次商业化应用。之后，又相继推出门禁、汽车防盗、汽车遥控钥匙、物流和公交等多种产品，涉及 125kHz（低频）、13.56MHz（高频）、860～930MHz（超高频）和 2.45GHz（微波）等多个频段。

3. 双界面卡

双界面卡就是将接触式接口和非接触式接口集合在同一实体上的 IC 卡。

4. 物联网

1999 年在美国召开的“移动计算和网络”国际会议上提出物联网概念：在计算机互联网的基础上利用 RFID 技术、无线数据通信技术和物品的电子编码 EPC，构造出实现全球物品信息实时共享的物联网。后来对物联网的定义和应用范围又做了大的扩展，不仅限于 RFID 标签，还包括各种信息传感设备，如传感器、全球卫星定位系统（GPS）等，实时采集需要监控的信息或移动物品的位置等。

1.6 智能卡与 RFID 标签的架构

当前 IC 卡的应用已普及推广，RFID 标签的应用也逐步发展，由于 IC 卡的设计、制造和应用各方面都已成熟，因此下面首先介绍 IC 卡中性能较强、含有微处理器的接触式

智能卡，然后再介绍非接触式 IC 卡和 RFID 标签。

1. 接触式 IC 卡的架构

IC 卡和读写器之间完成数据和控制信息的双向传输。卡上的 8 个触点是读写器向 IC 卡提供电源、信号命令、数据及 IC 卡向读写器返回数据与状态的触点。持卡人使用 IC 卡时，需在卡内完成的操作已有相应的国际标准规定，以达到 IC 卡在一定应用范围内可用的目的，甚至可在全国或国际上使用。

每次使用接触式 IC 卡时，在一般情况下，持卡人以及卡与读写器之间自动执行的操作步骤如下。

1）持卡人向读写器插入 IC 卡

读写器接收到卡插入的信息后，按一定时序向 IC 卡的各个触点提供电源、复位信号和时钟信号等，以满足卡内电路、微处理器、存储器等的需要。

2）IC 卡向读写器返回复位应答信号

复位应答信号包括 IC 卡发行者的标识符及卡支持的一些基本参数。

如果读写器不支持该卡和发行者标识或存在某些错误，将停止操作，否则进入步骤 3）。

3）读写器向 IC 卡发出命令

IC 卡对命令进行处理后，向读写器返回数据（如果该命令要求返回数据）和处理状态，后者表示该命令是执行成功还是存在错误而失效。

然后继续执行下一条命令，直到完成本次使用的全部功能。

从安全角度出发，在步骤 3）中一般按以下顺序操作。

（1）读写器与 IC 卡相互认证对方是否合法。

（2）持卡人输入密码（PIN），验证持卡人身份的合法性。

（3）实现应用所需的功能。

上述每一步都由若干条命令组成的子程序完成。

在国际标准 ISO/IEC 7816 中定义了各条命令能完成的功能，但是在卡内，微处理器指令能完成的功能与它差别极大，为此在卡内设计了操作系统，通过微处理器执行各段子程序完成 IC 卡中的各条命令的功能，是操作系统的主要内容之一。

4）完成操作

由于使用 IC 卡的一次操作已经完成，于是读写器按一定顺序撤销向 IC 卡提供的电源、时钟信号等。

5）拔卡

持卡人将卡拔出，或者读写器自动将卡退出。

2. 非接触式 IC 卡和 RFID 的架构

当非接触式 IC 卡在读写器发射的磁场空间时，依靠卡内设置的天线和射频空中接口获取能量（形成电压）和信息。由于在磁场空间可能存在多张非接触式 IC 卡，因此产生信息冲突现象，与接触式 IC 卡相比，为了防止冲突，增设了一部分专用命令，从而实现了场内多张 IC 卡逐张处理的功能。RFID 标签采取相似的措施解决冲突问题。

1.7 本书的内容简介

本书的第 1 章为概论，对智能卡(从芯片到系统)和 RFID 标签及读写器做了简明的描述，并介绍了物联网的概念，突出了卡的安全问题和标准化问题。

第 2～14 章划分成以下 5 个阶段。

1) 物联网和智能卡的技术和应用的基础知识和实施(第 2～5 章)

第 2 章：对数字逻辑电路、计算机和互联网进行简明的介绍。

第 3 章与第 4 章：对卡和标签中可以采用的数据和文件的表达方式及实际应用的数据进行了定义，并说明了接触式 IC 卡与读书器之间的触点功能。

第 5 章：安全和鉴别。

2) IC 卡的硬件架构和操作系统(第 6、7 章)

第 6 章：智能卡的命令系统。

第 7 章：IC 卡芯片和卡内操作系统。

3) 射频识别技术和 IC 卡、RFID 标签的空中接口(第 8～10 章)

IC 卡、RFID 标签及通信设备等都从有线向无线连接方面发展，且是物联网应用的基础设备。前面论述的内容(除了卡与读写器之间的触点外)均适用于无线连接的设备。

第 8 章：射频识别技术。

第 9 章：非接触式 IC 卡国际标准 ISO/IEC 14443 和 ISO/IEC 15693。

第 10 章：RFID 标签空中接口标准 ISO/IEC 18000 系列。

4) 读写器结构及系统的测试(第 11 章)

第 11 章：读写器的组成与结构，以及卡与读写器的测试。

5) 互联网、物联网的应用和创新，三网融合(第 12～14 章)

第 12 章：物联网的技术基础、“互联网＋”和云计算。

第 13 章：三网融合(互联网、电信网、广播电视网)。

第 14 章：物联网和智能卡的应用。

习题

1. 计算机和互联网的作用是什么？
2. 什么是智能卡和 IC 卡？
3. 什么是信用卡和现金卡？
4. 接触式和非接触式 IC 卡的主要区别是什么？
5. 非接触式 IC 卡和 RFID 标签的主要区别是什么？
6. 简要说明计算机网络在 IC 卡工程中的重要性。
7. 智能卡与安全有什么关系？
8. 卡内操作系统的作用是什么？

9. PIN 主要用于验证持卡人的身份、保护卡主人的利益，这种说法对吗？
10. 一个现代化的信用卡应用系统的硬件应包括哪些主要部件和设备？
11. 什么是读写器？其功能是什么？是否允许商店的雇员对读写器进行改装？
12. 物联网是怎样定义的？简述物联网和互联网的关系。
13. 国际标准、国家标准和工业标准的应用范围有什么差别？

第 2 章　计算机、互联网

计算机和互联网的基础知识已在大学的所有理工科专业得到普及。为了便于阅读本书，本章对计算机和互联网的有关内容进行复习或补充。

2.1　计算机系统

1946 年世界上第 1 台电子计算机在美国陆军部资助下研制成功，几年后，冯·诺依曼(von Neumann)与莫尔小组合作研制了称为 EDVAC 的计算机。其后世界上研发的计算机虽然在技术、速度、性能和应用上不断飞跃前进，但其最基础的实现原理仍与 EDVAC 保持一致。

当计算机中采用的电子器件由电子管不断向晶体管、集成电路、超大规模集成电路发展时，计算机的性能不断提高，体积不断缩小，价格不断下降。在 20 世纪 60 年代中期生产了成本低而功能不是太强的小型计算机，掀起了计算机普及应用的浪潮，在工业、企业和控制领域中发挥作用。20 世纪 70 年代后期出现的微型机掀起了个人应用计算机的普及浪潮，1981 年 Intel 公司的 80386 微处理器问世，除了提高主频和运算速度外，还将原属于芯片外的有关电路(如浮点运算部件)集成到芯片内，Intel 公司的微处理器和微软公司的操作系统组成的微机成为主流产品。目前高性能微处理器芯片(超大规模集成电路)所含的晶体管数可达几十亿个，计算机向高性能和普及应用两个方向发展，为了便于个人携带，微型机向笔记本电脑、平板电脑发展，而且信息的有线传送和无线传送兼顾，计算技术和通信技术的结合产生了智能手机。尤其是将地理上分散的多台可独立运行的计算机通过软、硬件的配合和互联，实现信息交换、资源共享(存储和计算)、协同工作等功能，从而实现了到处可见的计算机网络。

2.1.1　计算机组成

1. 框图

图 2.1 所示为早期计算机的框图。

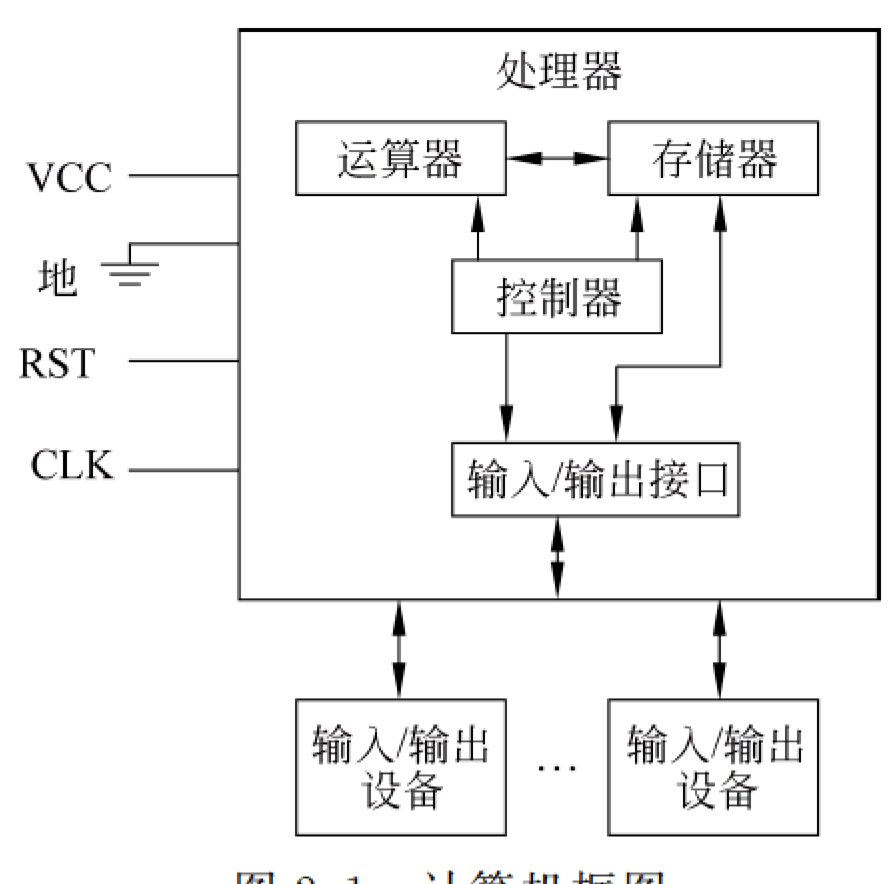


图 2.1　计算机框图

计算机由运算器、控制器、存储器和输入/输出设备组成。应用时，由输入设备输入信息(包括数据和程序)，信息一般存放在存储器中，然后对程序和数据进行处理(算术逻辑运算在运算器中进行)，最后将结果输出，所有操作都在控制器控制下进行。

在图中，VCC 为电源的接入点，RST 为 reset 的缩写(让处理器进入工作的初始状态)，CLK 为

时钟。

2. 指令系统

在计算机中，设计有若干条指令，其集合称为指令系统，每条指令完成指定的操作。根据应用需求，顺序执行编写好的一串指令(称为程序)，完成预定的功能。

最简单的指令系统包括算术逻辑运算指令、数字移位指令、程序转移指令和输入/输出指令。随着集成电路工艺的改进，运算速度的提高，应用范围的扩大和复杂程度的增强，指令系统中包含的指令数量不断增加，其中相当多的指令完成的功能也增加了。从而增加了设计的难度、成本和产品推出的时间，后来称这种计算机为复杂指令系统计算机(Complex Instruction Set Computer，CISC)。

对 CISC 进行测试表明，各种指令在程序中的使用频率相差悬殊，最常使用的是一些比较简单的指令，仅占指令总数的 20%，在程序中出现的频率却占 80%；而占 80%的复杂指令在程序中的频率仅占 20%。对指令系统合理性研究结果，导致了精简指令系统计算机(Reduced Instruction Set Computer，RISC)的诞生，除了简化指令系统外，还对计算机的结构进行改进，在智能卡、电路设备和工业控制等领域，一般使用 RISC 指令系统。

当前，高档的 CISC 计算机的主要设计和生产单位是美国 Intel 公司。RISC 的设计单位是英国的 ARM 公司，现已被日本软银集团收购。

2.1.2 操作系统

早期，计算机的使用者必须用二进制数字码表示的指令编写程序，称为机器语言；在 20 世纪 50 年代出现了用符号表示的指令来编写程序，称为汇编语言。用这两种语言编写应用程序工作量很大，并且容易出错，要求编写应用程序的技术人员对计算机的硬件和指令系统有正确、深入的理解，专业知识丰富，编程技术熟练。

为了管理计算机各部件的工作，开发了管理程序，后来发展为计算机操作系统和网络操作系统。操作系统合理地组织计算机的工作流程和数据的处理，管理和分配存储空间，控制和管理输入/输出设备，并提供良好的使用界面，方便用户使用计算机。

操作系统是由系统程序员编写的程序，在显示屏幕上提供基于图形和文字的人机交互界面，方便应用程序的编制或计算机的使用。

图 2.2 所示为多层次结构的计算机系统。计算机硬件是实际存在的机器，配上操作系统后就称为虚拟机，对应用程序员来说，编写程序时并不需要了解计算机硬件。计算机系统如图 2.2(a)所示。目前存在多种操作系统，对微机来说，有基于 Windows、Linux 等的操作系统。

不同公司设计的操作系统所完成的功能和提供给应用程序的界面都不相同，为了便于应用程序的开发和应用程序在不同机器之间的可移植性，期望能在操作系统之上形成一个标准化的平台(或称为中间件)，如图 2.2(b)所示，增加了一个层次。一般在平台上提供应用程序编程接口(Application Programming Interface，API)，供第三方应用程序 APP 开发人员使用，APP 是 Application 的缩写，在平板电脑和智能手机屏幕上都有不少 APP，如计算器、日历、相机、腾讯新闻 HD、腾讯微信、百度 HD、京东 HD 等图标供个人选择。

HD(High Definition)是高解析度的意思，表示高清电视、高清设备或高清格式。通

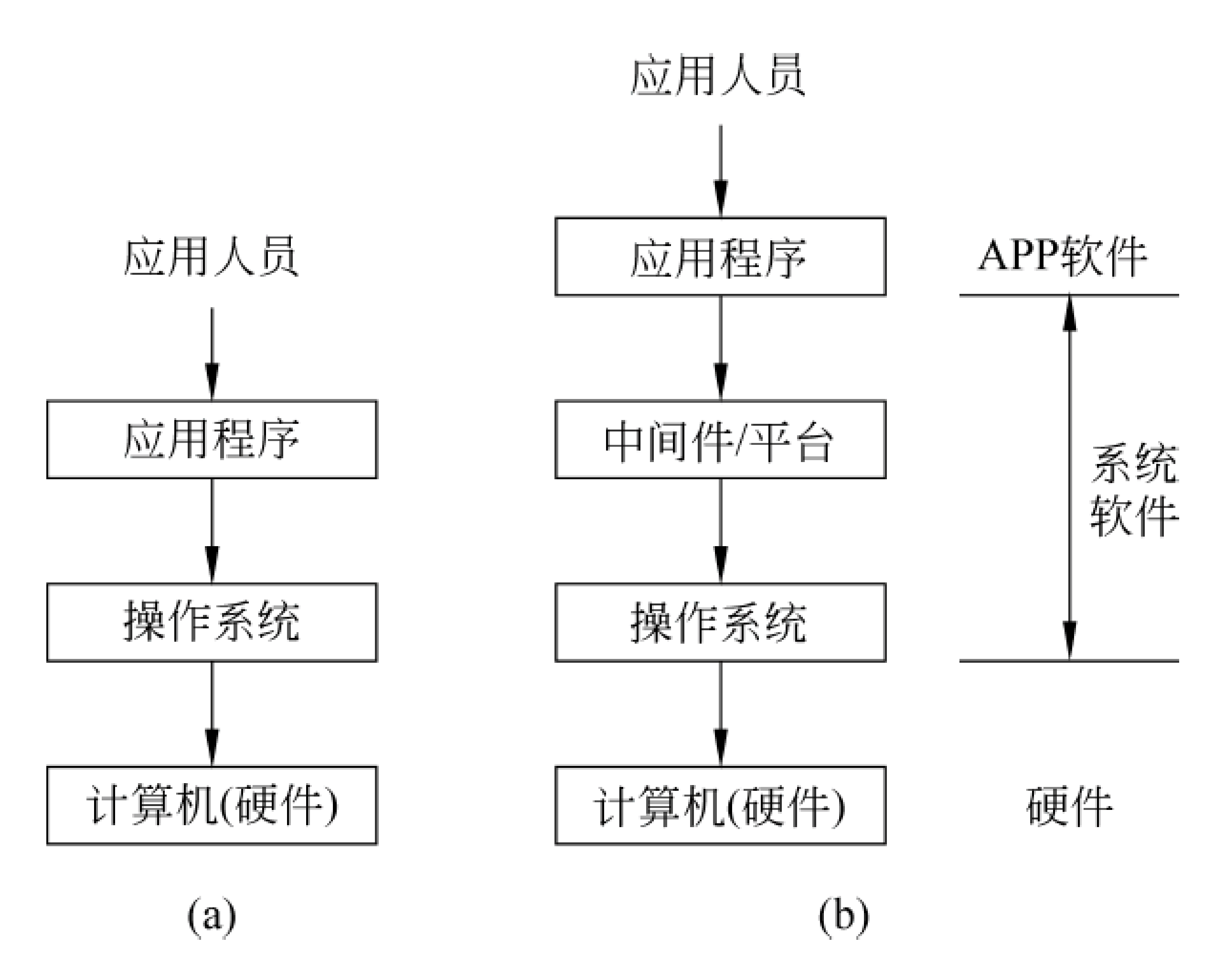


图 2.2　多层次计算机系统

常在平板电脑的应用上用 HD 标识，或者忽略 HD 两字。

2.1.3　数字逻辑电路

数字电子计算机的硬件都由数字逻辑电路构成，数字电路用高电位/低电位两种状态来表示数字 1 和 0（或 0 和 1）。

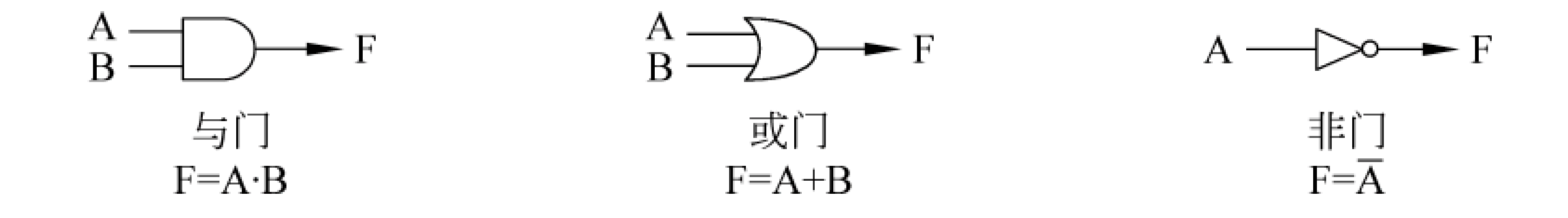
数字逻辑电路分为以下两类。

1. 组合逻辑电路

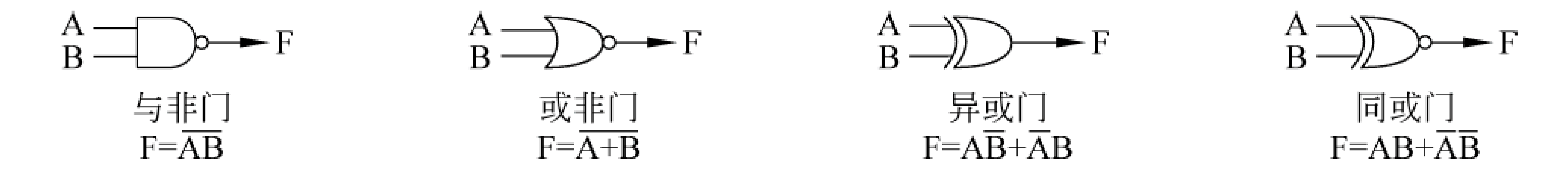
组合逻辑电路是指电路的输出仅与当前的输入状态有关，而与以前的输入状态无关。基本上有“与门”“或门”和“非门”3 种电路，并可组合成各种功能模块。在国际上常用的有以下两种标准。

1）ANSI/IEEE Std 91-1984

门电路采用“形状特征型”符号来表示，假设有两个输入信号 A 和 B，其输出为 F，逻辑图和逻辑运算公式表示如下：



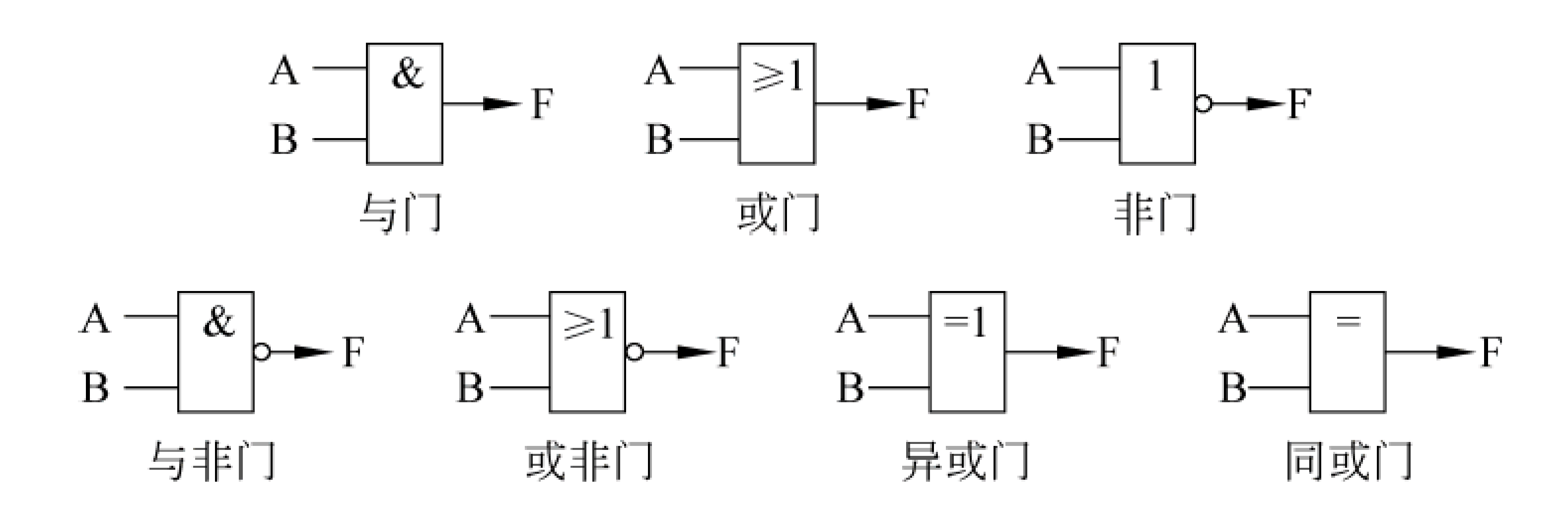
多个门组合后，形成常用的逻辑电路，表示如下：



异或门可完成算术加法运算，得出结果，未考虑“进位”，称为半加器。

2）IEC 60617-12

门电路采用“矩形”符号来表示其逻辑图和逻辑符号如下。



我国的国家标准采用“矩形”符号，但在国际上更多采用的是“形状特征型”符号，在本书中一般采用“形状特征型”符号。

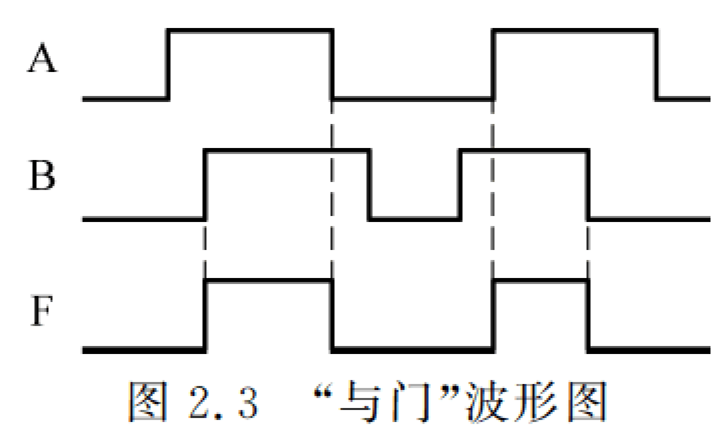


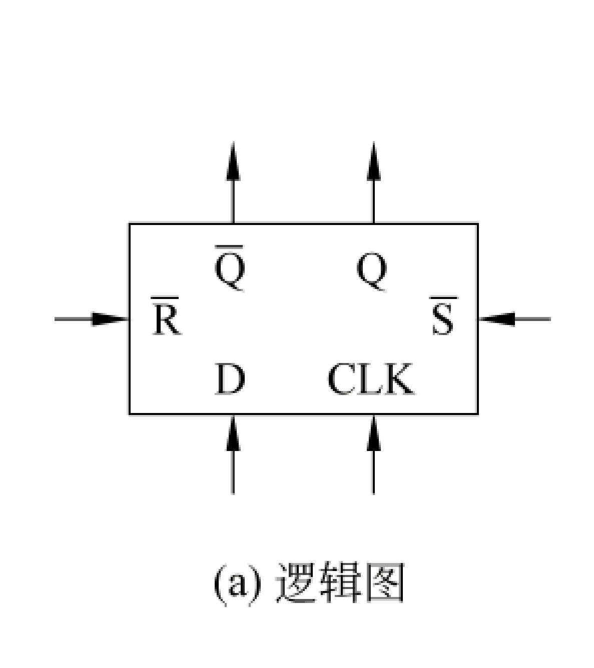
图 2.3 “与门”波形图

上面讨论的以两个输入端电路为例，一般不超过 5 个输入端。A 与 B 可以都是数，也可以作为控制信号，假设在“与门”中 A 为数，B 为控制信号，则当 B=1 时，将门打开，F=A；当 B=0 时，将门关闭，F=0，由此形成选择器、译码器等多种组件。

图 2.3 所示为“与门”的输入信号和输出信号的波形图。当 A、B 均为 1 时，F=1，为其他输入时，F=0。

2. 时序逻辑电路

时序逻辑电路是指电路的输出与当前的输入和时序信号(图 2.1 中的 CLK)有关，而且时序电路中必须要有存储信息的记忆元件——触发器。时序逻辑电路有多种类型的触发器，下面以 D 型触发器为例进行讨论，如图 2.4 所示。



(a) 逻辑图

$\overline{R}$	$\overline{S}$	CLR	D	Q	$\overline{Q}$
0	1	X	X	0	1
1	0	X	X	1	0
1	1	↑	0	0	1
1	1	↑	1	1	0

(b) 功能表

(c) 波形图

图 2.4 D 型触发器

在图 2.4(a)中，D 为输入数据，Q 与 $\overline{Q}$ 为输出数据，$\overline{R}$ 为触发器的清“0”信号，$\overline{S}$ 为触发器的置“1”信号，时钟 CLK 的上升沿将数据 D 存储于触发器中，图 2.4(b)中的“X”表示不影响输出，在图 2.4(c)中假设 Q 的初始状态为“1”。

多个触发器可组成多位寄存器，在 CLK、$\overline{R}$、$\overline{S}$ 的配合下，输出 Q 可以保持原值不随输入数据 D 而变化，因此被说明有记忆功能。

3. 计算机与外界的联系

在图 2.1 中，与外界联系的有电压、地、信号(RST、CLK)、输入/输出(I/O)和数据线。

(1) RST。又称为复位信号，加电时，触发器的状态(1 或 0)不能预知，这是因为 D 型触发器一般由 6 个门组成，其中各个晶体管在加电时的工作特性不完全一致而造成状态

的不确定。RST将某些相关的触发器或控制信号设置成初始状态，以保证计算机正常运行。

RST可由外界提供，或者加电时在机内自动产生，前者称为冷复位，后者称为热复位。

(2) CLK时钟。由计算机内部的晶体振荡器自动生成，或者由外界输入的脉冲，按一定的时间间隔(称为周期)重复出现。

(3) I/O(输入/输出)接口。根据应用需要，通用计算机或微机可能拥有键盘、打印机、显示屏、闪存等。I/O设备有时称为外部设备。

根据外部设备功能的不同，计算机与外部设备之间有按位顺序传送数据和多位并行传送数据两种方法。

接触与非接触IC卡都采用按位顺序传送数据的方法。

传送数据的有线接口称为通用串行总线(Universal Serial Bus，USB)，无线传输在空中进行，将在后面章节中详细说明。

计算机或微机之间通过网络相联，有"网络就是计算机"的说法，在本书中将对互联网中的局域网(以太网和WiFi设备)进行讨论。

4. 逻辑电路功能举例

(1) 寄存器。每个触发器可存储一位二进制数(0或1)，寄存器由多个触发器组成。例如，字长为16位的寄存器由16个触发器组成，并加上控制电路接收数据。根据功能的不同，配以相应的控制电路可组成移位寄存器等。

(2) 处理器。在图2.1的处理器中，除存储器外，都可用数字逻辑电路实现，假如指令系统比较简单，则完成相同功能的操作系统比较复杂。

(3) 阵列逻辑电路。"阵列"是指逻辑电路在芯片上以阵列形式排列(与阵列、或阵列)，有多种型号，有的芯片上还有触发器。根据用户需要可对阵列中门电路进行互联(或称为编程)，以实现所需的功能。有的则一次设定后不允许再改变。上述阵列逻辑电路统称为可编程序逻辑器件。

现场可编程序门阵列FPGA由大规模集成电路构成，内有重构逻辑的程序存储器将用户所需实现的逻辑以某种程序形式从片外输入到重构逻辑的程序存储器(程序由厂商提供的开发系统生成)，可以允许用户多次修改逻辑电路，程序修改也很方便，适合在产品试验或生产批量不大时使用。

2.1.4 IC卡与外界的联系、智能卡命令中的逻辑通道

1. 接触式IC卡与外界的联系

智能卡与外界的联系有电压、地、RST、CLK和I/O端口，与图2.1的区别是仅有一个外部设备(读写器)。在卡内部，将处理器和操作系统集成在一个芯片内，称为片上系统，完成读写器发出的命令所指定的功能。

逻辑加密卡内部功能全部由逻辑电路完成，没有处理器和操作系统。

2. 微处理器的多核芯片和智能卡的逻辑通道

随着超大规模集成电路技术的发展，有几亿量级的晶体管可集成在单个芯片中，于是

出现了可在一个芯片内集成两个或更多的处理器，称为物理处理器核。而且每个物理处理器核在操作系统控制下可实现若干个逻辑处理器功能。前面介绍的计算机是实际存在的物理处理器，而逻辑处理器是指软件执行多道程序(多线程)的虚拟处理器。例如，Intel公司推出的酷睿(Core)i7 微处理器实现了 4 核/8 线程，即一个芯片内集成了 4 个物理处理器核，每核可运行两个线程，相当于两个逻辑处理器。为了实现多核功能，对指令系统中的某些指令进行相应的处理。

IC 卡内的处理器功能比较简单，不会使用多核芯片(在其他很多应用场合会用到)。在此希望读者理解“物理”和“逻辑”的差别，从而可解释下面提到的逻辑通道号。

在第 6 章智能卡命令系统中，每条命令都指出执行本条命令时的逻辑通道号，总共有 4 个通道或 16 个通道，可理解为与程序有关的虚拟通道号，不同通道中执行的程序是相互独立的。在卡内仅存在一个物理通道，但可以实现一个逻辑通道或多个逻辑通道的功能。

2.2 计算机网络

2.2.1 计算机应用的 4 个阶段

(1) 早期的计算机由于价格昂贵、体积庞大，与当时的其他计算工具相比，可称之为大型机。除了军用以外，大型机安装在计算中心，并设置多台终端，供多个用户使用。计算机内运行的软件是分时操作系统，即将计算机硬件的运行时间分成多个时间片，提供给当时在机房内的用户分时使用。

(2) 小型机和微型机的出现满足了一个单位或个人使用一台计算机的愿望，提高了计算机的普及程度。但是计算能力、数据、资源和外部设备的配置等不能满足某些科研、设计和应用单位的需求，于是萌发了将多台小型机或微机相互连接实现资源共享等目的，推动了计算机网络技术的发展。

(3) 局域网。如果一个科研设计单位、一个实验室、一个教学楼或一个办公大楼内有多台计算机，将它们互联起来，实现资源共享，这就是局域网，一般在局域网中设置服务器，为共享资源服务。

根据计算机之间的相隔距离不同，分为局域网、城域网和广域网。其中，主要应用的是局域网和广域网。

(4) 广域网。目前覆盖全球范围且广泛应用的网络是因特网(Internet)，是通过路由器实现多个广域网、局域网，甚至个人计算机互联的大型网际网，是一个全球范围的信息资源网，通过应用程序的开发，完成金融、商务、政府、科研、医疗卫生、电子书刊和游戏等各方面的应用。

2.2.2 互联网

1969 年美国国家科学基金会(NSF)、能源部、美国国家航空航天局(NASA)把下属单位的网络连接起来，组成 ARPANET 网，经过推广和发展产生了。在全球范围应用的

Internet，音译为中文“因特网”。凡是由能彼此通信的设备组成的网络称为互联网，其英文名字为 internet，首个字母是小写 i。因特网是互联网中的一种。

Internet 使用的是 TCP/IP。

1. TCP/IP 体系结构

计算机网络主要解决计算机之间的数据传输问题，即数据能迅速可靠传输到目的地（计算机）。图 2.5 所示为 TCP/IP 的层次结构图。

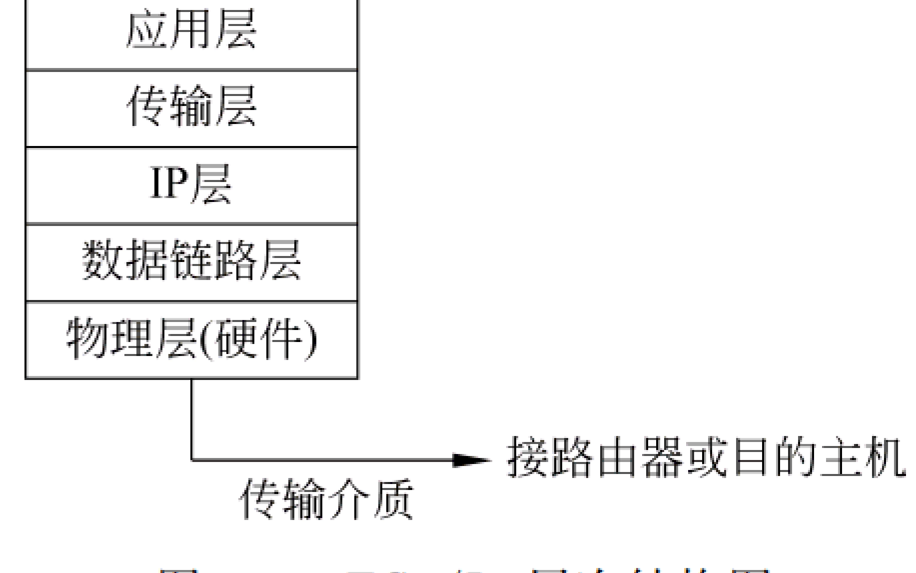


图 2.5　TCP/IP 层次结构图

(1) 应用层。应用层在最高层，用户调用应用程序来访问互联网提供的多种服务，负责向传输层发送数据和从传输层接收数据。下面主要讨论下层如何发送数据。

(2) 传输层。传输层提供可靠的传输服务。传输层将传送到的数据流划分成分组（称为数据报），每个数据报写上顺序号，并连同目的地址传送到 IP 层，确保数据无差错地按顺序到达。

(3) IP 层。IP 层使用路由算法得出是直接将数据报传送到目的地（主机），还是传送给路由器的控制信号。而且还要处理接收到的数据报，检验其正确性。

(4) 数据链路层。数据链路层负责接收 IP 数据报，实现介质访问控制功能（多个数据发送源的冲突问题），将数据送到物理层。

(5) 物理层。物理层协调在物理介质上传输数据所需的功能。

常用的传输介质有双绞线、同轴电缆、光纤和无线传输（无线空中传输）。

接收数据是发送数据的逆过程，从物理层接收数据，并逐层向上传输到应用层。

2. TCP/IP（数据传送功能）

TCP 是传输控制协议，IP 是网间协议。数据传送过程完成的功能如下。

(1) 首先由 TCP 把传送数据分成若干数据报（数据报是一个基本传输单位），并写上序号。

(2) IP 给每个数据报写上发送主机和接收主机的地址，并进行路由选择。

(3) 在物理网上传送数据。

说明：数据报可能通过不同途径（路由选择）进行传输，接收主机可能发现接收的数据报序号不顺、数据丢失、数据失真或重复传输现象，这些问题都由 TCP 解决，纠正错误或请求重发。所以可总结为 TCP 负责数据的可靠传输，IP 负责数据传输途径。

3. Internet 地址

Internet 地址又称为 IP 地址，网上每台计算机或每个用户都有一个全球唯一的地址，用来区别网上所有的计算机和用户。IP 有 IPv4 和 IPv6 两个版本。

(1) IPv4 地址。分配给每台主机一个 32 位数作为主机 IP 地址，在发送的数据报中都包含了 32 位发送方地址和 32 位接收方地址，用点号分隔的 4 个十进制数字表示。例如，166.111.16.5 是某台指定计算机的 IP 地址。允许人们用字母和数字混合表示计算机地址，要求不发生重名现象。同时 Internet 提供了一种服务，将它翻译成十进制数表示的 IP 地址。

由于预先设定的 IP 地址分配方案不完全理想，因此快速增长的地址请求会出现不能

满足的现象，于是制定了 IPv6 地址协议。

（2）IPv6 地址。地址长度为 128 位，它含有的地址数是 3.4×10^{38}，能够为所有可以想象出的网络设备提供一个全球唯一的地址。128 位地址被划分为 8 个 16 位部分，每部分用十六进制数表示。

IPv4 和 IPv6 会同时存在一段时间，IPv6 包含了给 IPv4 使用的地址空间。

4. 互联网的应用

互联网是属于全人类、全球性的网络，所有不同的计算机和操作系统都可以连接互联网。全球有一个固定机构来为每一台主机命名（即地址）。在技术层面，不存在某国或某利益集团通过技术来控制互联网，也无法将互联网封闭在一个国家内。互联网的管理与“服务”有关，而与“控制”无关。

现代社会中存在着计算机网络、电信网络（移动通信）和有线电视网络，随着互联网的广泛应用，三者在结构、技术和服务领域紧密融合。

计算机网络的 IP 技术，可以将传统的电信设备变为互联网设备，移动通信（3G、4G）技术将数据业务带入移动计算时代，数据通信量和服务内容急剧增长。

互联网在军事、政务、商务、工业等领域得到广泛应用，为科研、应用、产业的发展产生深远影响，并利用 IC 卡、RFID 标签、传感器等采集数据，形成物联网。从而提出了“大数据”“云计算”和“互联网＋”的概念和实施前景。

习题

1. 在运算器中进行算术运算（加、减、乘、除）至少要用到哪些逻辑电路？
2. 设计使用 D 型触发器和门电路组成的一位计数器和二位计数器。
3. 简述逻辑加密卡和 CPU 卡中用到的数字逻辑电路的主要区别。
4. 是非题（仅回答“是”或“否”）：
   ① 设计微处理器时，一定考虑设计指令系统。
   ② 微处理器通过执行程序才能完成预定的功能。
   ③ 设计操作系统的公司，务必完成所有应用程序的设计。
   ④ IC 卡和读写器内部一定含有微处理器。
   ⑤ 当前银行发行的金融卡一定有互联网支持。
5. TCP/IP 主要完成什么功能？
6. 猜猜看：你手中的卡哪些是磁卡、逻辑加密卡，哪些是智能卡？
7. 简述“物理”与“逻辑”的意义和区别。
8. 简述“硬件”和“虚拟机”的意义和区别。

第 3 章　IC 卡信息编码（数据元、数据对象和文件）

IC 卡的流通范围很广。例如，银行卡可以在国内或国际范围内流通，交通卡可以在一个城市或跨区域范围内使用。为了便于识别、阅读和检索 IC 卡中存放的各种信息（数据），从而制定了编码规则。按各种数据的内容、性质或用途的不同，对其进行分析、划分归类，给出不同的标记，并纳入国际标准中，以促进 IC 卡的流通使用。

在本章中提到的 IC 卡即为智能卡。

在 IC 卡中存储的信息可归纳为数据元、数据对象和文件 3 种。

在 IC 卡和读写器之间的接口处所见到的最小信息项（如一个名称、逻辑描述符、格式编码等）称为数据元（Data Element，DE），而在接口处所见到的由标记 T（Tag）、长度 L（Length）和数值 V（Value）字段组成的信息称为数据对象（Data Object，DO）。在 IC 卡中，数据对象一般按照国际标准 ISO/IEC 8825-1 中定义的基本编码规则（Basic Encoding Rules，BER）进行编码。

文件内存放控制信息和应用数据（由数据元和数据对象组成）。

3.1　基本编码规则（BER）

3.1.1　编码结构（BER-TLV）

数据对象 DO 的编码由标记 T、长度 L 和数值 V 三部分组成，其中标记和长度是为了解释数值部分而引入的。每部分由一个或若干字节组成，每个字节包含 8 位二进制数 $b_8 \sim b_1$，b_8 为最高位，b_1 为最低位。

标记 T	长度 L	数值 V

1. 标记 T

标记 T 表示数据对象的类别（4 个标记类别、两个编码类别）和标记编号，由一个或多个字节组成，首个 8 位字节安排如下（图 3.1）。

（1）b_8、b_7 表示标记类别，$b_8b_7=00$ 为通用类，$b_8b_7=01$ 为应用类，$b_8b_7=10$ 为上下文相关类，$b_8b_7=11$ 为专用类。

（2）b_6 表示编码类别，$b_6=0$ 为原始编码（P），$b_6=1$ 为结构化编码（C）。

（3）$b_5 \sim b_1$ 为标记编号，如果编号范围在 0～30（二进制 0000～11110），则表示标记 T 为 1 字节，如图 3.1 所示；如果 $b_5 \sim b_1=11111$，则表示标记 T 为多个字节，其编号不小于 31。当后继字节的 b_8 为 1 时，表示后面还有后继字节；当 b_8 为 0 时，表示该字节是 T 的最后一个字节，如图 3.2 所示。标记的编号由后继字节的 $b_7 \sim b_1$ 链接而成。

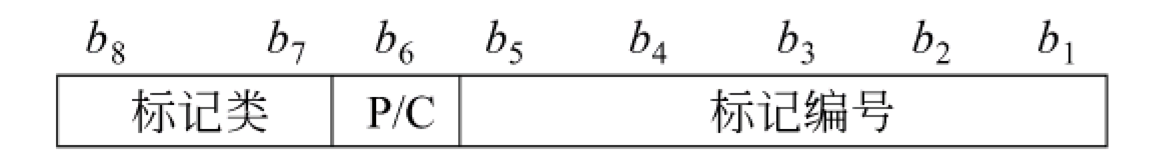


图 3.1　标记 T(编号 0～30)

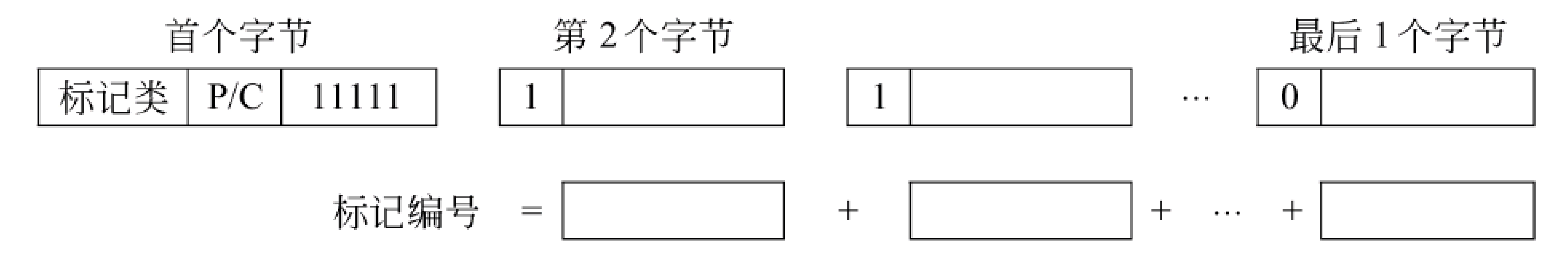


图 3.2　标记 T(编号由多个字节组成)

由此得出数据对象的 4 种标记类别的编码范围如表 3.1 所示。

表 3.1　数据对象的 4 种标记类别的编码范围(由第 1 个字节表示)

b_8 b_7 类别	b_8～b_1 编码范围(十六进制表示,×为任意值)	
00 通用类	'0×'～'1×'(原始编码)P	'2×'～'3×'(结构化编码)C
01 应用类	'4×'～'5×'(原始编码)P	'6×'～'7×'(结构化编码)C
10 上下文相关类	'8×'～'9×'(原始编码)P	'A×'～'B×'(结构化编码)C
11 专用类	'C×'～'D×'(原始编码)P	'E×'～'F×'(结构化编码)C

在本章中还用数据下标表示进位制,如十进制数 5_{10} 表示二进制数 101_2。

2. 长度 *L*

长度 L 由一个或多个字节组成。如果 L 的首个字节的 $b_8=0$,则 L 的长度为一个字节,b_7～b_1 表示数值 V 的字节数(≤127);如果 $b_8=1$,则 L 的长度为多个字节,b_7～b_1 表示后继长度的字节数,后继长度字节的内容为数值 V 的字节数。

L 的首个字节不使用 FF,FF 供将来扩展使用。

例如:

(1) $L=33_{10}$(十进制数 33),b_8～b_1 编码为 00100001_2(二进制数),$b_8=0$,L 的长度为一个字节。

(2) $L=201_{10}$,编码为 10000001_2 11001001_2,首个字节的 $b_8=1$,表示长度由多个字节组成;b_7～$b_1=0000001$,表示 L 后继字节的长度为 1。第 2 个字节为数值 V 的字节数 201_{10},$2^7+2^6+2^3+2^0=128+64+8+1=201_{10}$。

3. 数值 *V*

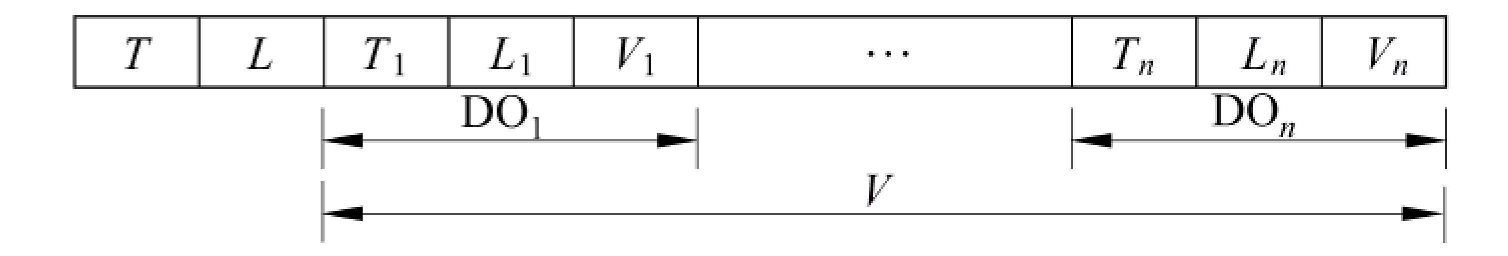
数值 V 由 0 个、一个或多个字节组成,有两种编码方式:数据对象 DO 的原始编码和结构化编码。这两种编码的主要区别是 V 字段的表示方法不同。

(1) 原始编码格式:

标记 T	长度 L	数值 V

前面介绍的编码格式即是原始编码格式。

（2）结构化编码格式：



其中，T 为标记，L 为 V 字段的长度，而 V 字段则由一个或多个数据对象组成，被称为 T 的模板（Template）。在模板中：

T_1、…或 T_n＝DO_1、…或 DO_n 的标记。

L_1、…或 L_n＝DO_1、…或 DO_n 的长度。

V_1、…或 V_n＝DO_1、…或 DO_n 的数值。

用 TLV 来描述数据对象，可以完整地表示出数值的含义、值的大小及数据对象长度。而且 TLV 的总字数可从其本身算出来。

在 IC 卡领域内，广泛采用 TLV 表达形式，当采用结构化编码格式，有多个数据对象链接时，数据对象之间可以不用分隔符（或称为定界符）。

3.1.2 通用类、应用类和上下文相关类的编码

通用类的编码在国际标准的编码规则中定义，应用类、上下文相关类由各行业自行定义。在本书中尚未涉及专用类。

通用类编码，其中已确定编号的标记 T 在国际上具有唯一性，不能再进行其他定义。举例如下：

1. 布尔值

原始编码：$T=01_{16}$。如果布尔值为假（False），数值应为 0；如果布尔值为真（True），数值应为任意非 0 值，如下表所示（在本例中，用 FF 表示非 0 值）。

标记 T（布尔）	长度	数值
01_{16}	01_{16}	FF_{16}

十六进制数据一位相当于二进制数据 4 位，在 IC 卡中一般定义为一个数据单元，一个字节包含两个数据单元。

在上例中，$T=01_{16}=\begin{matrix} b_8 & b_7 & b_6 & b_5 & b_4 & b_3 & b_2 & b_1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1_2 \end{matrix}$，其中 $b_8b_7=00$，属于通用类，$b_6=0$ 为原始编码，$b_5\cdots b_1=00001_2$，其值为 0～30，因此 T 为一个字节。长度 L 和数值各为一个字节。所以该数据对象的总字数为 3 个字节。

2. 序列值

结构化编码：$T=30_{16}$。

例如，要求顺序列出两个数据对象：名字 Smith 和布尔值为真，可编码如图 3.3 所示。

T（序列）	长度	数值		
30_{16}	$0A_{16}$	T（名字） 16_{16}	长度 05_{16}	数值 Smith
		T（布尔） 01_{16}	长度 01_{16}	数值 FF_{16}
1字节	1字节	10字节		

图 3.3　序列值的编码

注：一个字节可表示两位十六进制数据(0～9,A～F)或一个英文字母(A～Z),图 3.3 中的 Smith 占用 5 个字节。

3.2　IC 卡使用的数据对象

3.2.1　数据对象的格式

在 IC 卡中,增加了一种简单的数据对象,因此有 Simple-TLV 和 BER-TLV 描述的两种 DO。

1）Simple-TLV 数据对象

- T 字段：由一个字节组成。编码范围为 1～254,'00'和'FF'为无效编码。
- L 字段：如果由一个字节组成,编码范围为 1～254,以 N 表示。如果第 1 个字节是'FF',则 L 字段由 3 个字节组成,后继的两个字节表示数值字段长度,范围为 0～65 535,也以 N 表示。
- V 字段：如果 L 字段的 $N=0$,不存在数值字段,这是一个空值 DO;如果 $N>0$,数值字段由 N 个字节组成。

在 IC 卡的文件组织中,可以用 Simple-TLV 数据对象来描述一个记录。

2）BER-TLV 数据对象

3.1.1 节中描述的 BER-TLV 同样适用,有两种 DO 编码：原始编码和结构化编码。

在国际标准 ISO/IEC 7816 中,数据元一般出现在数据对象 DO 的数值字段中或不用标记也能表达其含义的场合。

3.2.2　数据对象的标记分配

表 3.2 给出了按标记数字次序排列的部分数据对象 DO。在表中仅有两个通用类 DO,标记为 01 和 30(布尔值和序列值)。其他均为 IC 卡应用类数据对象(不适用于其他行业)。

表 3.2　按数字次序排列的 DO

标记	数据元名称	引 用 标 准	长度	可引用的模板标记
01	布尔值	ISO 8825-1	1 字节	—
30	序列值	ISO 8825-1	1 字节	—
41	国家机构	ISO/IEC 7816-6	可变	—

续表

标记	数据元名称	引 用 标 准	长度	可引用的模板标记
42	卡发行者机构	ISO/IEC 7816-4	可变	—
43	卡服务数据	ISO/IEC 7816-4	1 字节	—
44	初始访问数据	ISO/IEC 7816-4	可变	66
45	卡发行者数据	ISO/IEC 7816-4	可变	66
46	预先发行的数据	专有	可变	66
47	卡能力	ISO/IEC 7816-4	可变	66
48	状态信息	ISO/IEC 7816-4	1、2、3 字节	—
4F	应用标识符	ISO/IEC 7816-5	可变	61/6E
50	应用标号	ISO/IEC 7816-5	可变	61/6E
51	路径	ISO/IEC 7816-4	可变	61
52	执行的命令	ISO/IEC 7816-4	可变	61
53	自由选择的数据	ISO/IEC 7816-4/5	可变	*
54	偏移数据元	ISO/IEC 7816-4	可变	—
59	卡终止日期	—	$n4$	66
5A	主账号(PAN)	ISO/IEC 7813，ISO 8583	n…19	6E
5B	姓名	ISO/IEC 7501-1	可变	65
5C	标记列表	ISO/IEC 7816-4	可变	—
5E	登录数据(专有的)	专有	可变	6E
5F20	持卡者姓名	ISO/IEC 7813	$n2$…$n6$	65
5F24	应用终止日期	—	$n6$	6E
5F25	应用生效日期	—	$n6$	6E
5F26	卡生效日期	—	$n6$	66
5F28	国家代码	ISO 3166	$n3$	66
5F2A	货币代码	ISO 4217	$a3$ 或 $n3$	6E
5F2B	出生日期	—	$n8$	65
5F2C	持卡者国籍	ISO 3166	$n3$	65
5F32	交易计数器	—	可变	6E
5F33	交易日期	—	$n4$ 或 $n10$	6E
5F34	卡顺序号	—	$n2$	66
5F35	性别	ISO 5218	1 字节	65

续表

标记	数据元名称	引 用 标 准	长度	可引用的模板标记
5F40	持卡者相片	—	$n1$	6C
5F41	元素列表	—	可变	—
5F42	地址	—	可变	65
5F46	定时器	—	2 字节	66
5F48	持卡者秘密密钥	—	可变	65
5F49	持卡者公开密钥	—	可变	65
5F4A	认证机构的公开密钥	—	可变	65
61	应用模板	ISO/IEC 7816-4	可变	—
62	FCP 模板	ISO/IEC 7816-4	可变	—
64	FMD 模板	ISO/IEC 7816-4	可变	—
65	持卡者数据	—	可变	—
66	卡数据	—	可变	—
6F	FCI 模板	ISO/IEC 7816-4	可变	—
73	自由选择的数据	ISO/IEC 7816-4	可变	*
7D	安全报文模板	—	可变	—
7F20	显示控制	—	可变	66
7F21	持卡者证明书	—	可变	65

*：本表中定义的所有模板。

表中的符号所表示的意义如下。

- a：字母字符。
- n：数字，BCD 编码(二进制编码的十进制数)。
- s：专用字符。
- …：在两个数之间表示值的范围。

例如：

$a3$ 表示 3 个字母字符。

n…3 表示最多 3 个 BCD 码。

$n2$…4 表示 2、3 或 4 个 BCD 码。

表 3.2 中的标记由一个或两个字节组成，如果第 1 个字节的 $b_5 \sim b_1$ 为 11111(表中的 5F)，则表示标记为两个字节。

表 3.2 中提及的模板标记对应的数据如下。

标记 61——应用模板。

标记 65——与持卡者相关的数据。

标记 66——卡数据。

标记 67——鉴别数据。

标记 6E——与应用相关的数据。

例如，在标记为 61 的结构化 DO 模板中，可包含表 3.3 中所示的内容，该表是根据表 3.2 列出的。

表 3.3　应用模板——标记 61

标记	长度	数　据　元	标记	长度	数　据　元
4F	可变	应用标识符	53	可变	自由选择的数据
50	可变	应用标号	73	可变	自由选择的 DO
52	可变	执行的命令	51	可变	路径

3.2.3　编码举例

(1) 表示卡终止日期为 1995 年 2 月的 DO。

$$\underset{T}{\underline{59}}\quad\underset{L}{\underline{02}}\quad\underset{V}{\underline{95\ 02}}$$

(2) 表示应用终止日期为 1997 年 3 月 31 日的 DO。

$$\underset{T}{\underline{5F\ 24}}\quad\underset{L}{\underline{03}}\quad\underset{V}{\underline{97\ 03\ 31}}$$

(3) 表示个人出生日期的 DO。

$$\underset{T}{\underline{5F\ 2B}}\quad\underset{L}{\underline{04}}\quad\underset{V}{\underline{\mathrm{YYYYMMDD}}}$$（Y：年；M：月；D：日）

(4) 结构化的 DO 的举例。

$$\underset{T}{\underline{61}}\quad\underset{L}{\underline{0D}}\quad\underset{T_1}{\underline{4F}}\quad\underset{L_1}{\underline{05}}\quad\underset{V_1}{\underline{\mathrm{D}\times\times\times\times\times\times\times\times\times}}\quad\underset{T_2}{\underline{53}}\quad\underset{L_2}{\underline{04}}\quad\underset{V_2}{\underline{\times\times\ \times\times\ \times\times\ \times\times}}$$

标记 61 为应用模板，结构化 DO 中有两个原始编码；DO 分别是国家注册的应用标识符 AID[标记 4F(5 字节)]和自由选择数据标识符[标记 53(4 字节)]。

(5) 其他编码形式。

在 IC 卡中，某些数据元并不按 TLV 形式编码，如第 4 章中所讨论的复位应答、第 6 章中的命令编码等。由于它们出现在特定时间或场合，并由相关的国际标准予以详细的定义，因此不会产生二义性。

3.3　IC 卡的文件系统

3.3.1　文件的种类

文件用于管理应用和存储数据。每个文件都有文件名或文件标识符。

IC 卡支持两种文件：专用文件(Dedicated File，DF)和基本文件(Elementary File，EF)。

(1) 专用文件。专用文件是用于主持应用和有层次结构的文件。一个“应用 DF”(application DF)对应一种应用。“应用 DF”可以作为其他文件的父文件(是上层的文

件)，而其下层的文件被称为该 DF 的直属文件(可以是 DF 和 EF)。

(2) 基本文件。基本文件用于存放数据。EF 文件不能作为其他文件的父文件。EF 分为如下两类。

① 内部 EF：存储由卡内部使用的数据，即为了管理和控制目的由卡内操作系统所分析和使用的数据。

② 工作的 EF：主要存储外界可使用的数据，以及卡与读写器之间可相互传输的数据。

图 3.4 所示为双应用卡(应用 DF1 和应用 DF2)的文件层次结构。在这种卡的组织结构中，处于根部的 DF 称为主文件(Master File，MF)。所有 DF 可以是应用 DF(ADF)，也可以有其下层的 DF 和 EF。MF 可有其直属的 DF 和 EF，涉及卡的某些功能。图 3.4 中的 MF、应用 DF 都是专用文件 DF。

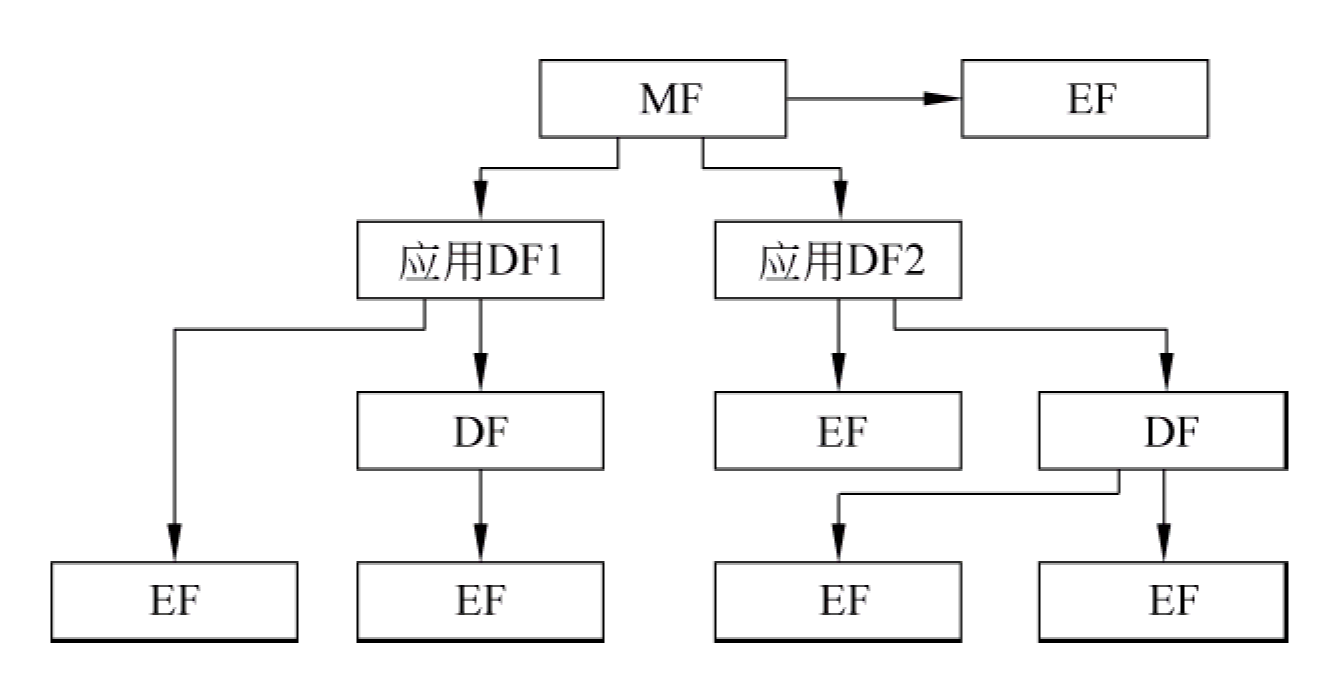


图 3.4　文件层次结构示例

3.3.2　文件选择方法、数据表示形式和文件控制信息

1. 文件选择方法

可利用以下 4 种方式之一来选择文件。

(1) 通过 DF 名选择。任何 DF 都可以通过按 1～16 个字节编码的 DF 名来选择。任何应用标识符(Application IDentifier，AID)均可作为“应用 DF”名。为了通过 DF 名进行无二义性的选择，“应用 DF”名在给定的卡内是唯一的。

(2) 通过文件标识符选择。任何文件都可以通过按 2 字节编码的文件标识符来引用。MF 的文件标识符已设定为'3F00'。为了通过文件标识符来无二义性地选择任何文件，在给定 DF 下的所有直接 EF 和 DF 都应具有不同的文件标识符。

(3) 通过路径选择。任何文件都可以通过路径来引用(一串文件标识符的链接)。该路径以 MF 或当前 DF 的标识符开始，并且以文件自身的标识符结束。在这两个标识符之间，路径由连续父 DF(如果有)的标识符组成。文件标识符的次序总是在父级至子级的方向上。

(4) 通过短 EF 标识符选择。EF 可以通过值在 1～30 范围内的 5 位(二进制)编码的短文件标识符(Short File Identifier，SFI)来引用。用作短 EF 标识符的值 0(即二进制的 00000)引用当前已选择的 EF。短 EF 标识符不能用在某些场合。

在 TLV 结构的数据对象中，如果标记 T 为'51'，其数值 V 即为文件或路径，可以是任

意长度。

2. 数据表示形式

在 DF 中,数据可能引用为数据对象。

在 EF 中,数据可能引用为数据单元、记录或数据对象,因此定义了以下 3 种 EF 结构。

(1) 透明结构。在 EF 中的数据可被看作一序列串联的数据单元。数据单元大小一般为 4 位二进制数或 1 字节。

(2) 记录结构。在 EF 中的数据可被看作一个可独立标识的记录序列,具有下列两种特点。

- 记录的长度:固定的或可变的。
- 记录的组织结构:按顺序(线性结构)或按环形(循环结构)。

(3) TLV 结构。在 EF 中的数据可看作一个数据对象集合。这些在 EF 中的数据对象是 SIMPLE-TLV 或 BER-TLV。

为引用 EF 数据,卡必须至少支持图 3.5 所示的 5 种结构中的一种。

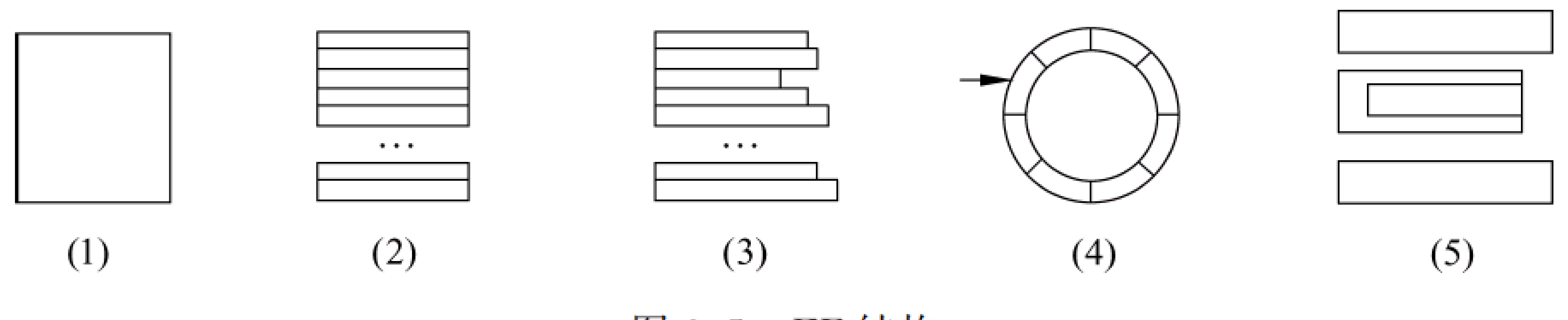


图 3.5 EF 结构

(1) 透明结构。

(2) 线性定长记录结构。

(3) 线性变长记录结构。

(4) 循环定长记录结构(箭头引用最近写入的记录)。

(5) TLV 结构(原始编码和结构化编码,在图 3.5(5)中,上部和下部为原始编码 DO,中间是结构化编码 DO)。

3. 文件控制信息

文件控制信息(File Control Information, FCI)可包含在任意 DF 或 EF 中,执行选择(SELECT)命令后可将被选中的文件设置为当前文件,并从文件中读出 FCI。该命令在第 6 章中说明。

表 3.4 所示为 3 种模板来嵌套文件控制信息 BER-TLV 数据对象。

表 3.4 与 FCI 相关的模板

标　记	值
'62'	文件控制参数(FCP 模板)
'64'	文件管理数据(FMD 模板)
'6F'	文件控制参数和文件管理数据(FCI 模板)

(1) FCP 模板。FCP 模板是文件控制参数(File Control Parameter，FCP)的集合，在表 3.5 中列出 FCP 模板中的部分内容，数据对象为上下文相关类(标记为'80'至'BF')，标记'85'和'A5'引用自由选择数据。

(2) FMD 模板。FMD 模板是文件管理数据(File Management Data，FMD)的集合，即数据对象为应用类，如应用标识符、应用标号和应用有效日期。在 FMD 模板中，标记'53'和'73'引用自由选择数据。

(3) FCI 模板。FCI 模板是文件控制参数和文件管理数据的集合。

表 3.5　文件控制参数 FCP(模板标记'62')的部分内容

标记 *T*	长度 *L*	值 *V*	适用于
'80'	变量	在文件中的数据字节数，不包括结构信息	任何 EF，1 次*
'82'	1 字节	文件描述符字节*	任何文件
'83'	2 字节	文件标识符	任何文件
'84'	1～16 字节	DF 名称	任何 DF
'88'	1 字节	短 EF 标识符	任何 EF，1 次
'8A'	1 字节	生命周期状态字节(LCS 字节)	任何文件，1 次
'8B'	变量	安全属性(见 6.2.1 节)	任何文件，1 次
'8E'	1 字节	通道安全属性(见 6.2.1 节)	任何文件，1 次
'AC'	变量	密码机制标识模板	任何 DF

* 文件描述符字节：说明是 DF 或 EF 文件，如果是 EF，则说明是 5 种结构中的哪一种。

* 1 次：表示该参数指定后不允许更改。

文件控制参数的表示方法举例：

T	L	T_1	L_1	V_1	T_2	L_2	V_2

T=62(FCP 模板)，L=7，T_1=83(文件标识符)，L_1=2，T_2=8A(LCS 字节)，L_2=1。

上例中，T_1=83，T_2=8A，是“上下文相关类”的数据对象，其含义与上文有关，此处的模板标记 T=62，是文件控制参数(表 3.4)，T_1=83，是文件标识符(表 3.5)。假如其上文是其他模板标记，比如在表 6.6 中，模板标记为 7D，83 是密文。其含义就不同了。以后(下文)就按其上文的定义处理。

下面对表 3.1 中的 4 种类别标记的唯一性进一步说明。

唯一性：例如，居民身份证号码具有唯一性，即每位居民的号码都不相同。银行卡的号码也具有唯一性，即没有两张卡的号码是相同的。

本行业的 4 种类型：

通用类标记(00～3F)：所有行业都适用，每个标记的含义不能改变，具有唯一性。

应用类标记(40～7F)：表 3.2 中的数据对象在本行业中适用，在其他行业另行定义，所以仅在本行业中具有唯一性。

上下文相关类(80～BF)：在本行业也不具备唯一性。

专用类（C0～FF）：未进行解释。

本章综述了智能卡中的信息编码（数据元 DE、数据对象 DO 和文件 DF、EF），为学习其后相关章节做准备，通过具体的应用，可加深对本章内容的理解。

习题

1. 试述数据元和数据对象的定义及两者之间的关系。
2. 原始编码和结构化编码数据对象的定义是什么？
3. 在结构化的 DO 中是否允许再套用结构化 DO？
4. 如果有两个 DO 链接如下：

   T_1-L_1-V_1- T_2-L_2-V_2

   其中不含有任何分隔符（或定界符），而且都用数字编码来表示，请问这两个 DO 的分界处是否可能混淆？
5. 如何得出表 3.1 中通用类 DO 的原始编码范围为'0×'～'1×'，结构化编码范围为'2×'～'3×'？
6. 在表 3.2 中，双字节标记 5F××是怎样产生的？如果有 5E××标记是否合理？
7. 上下文相关类数据对象有什么特点？其标记是否具有唯一性？具有唯一性标记的是哪类数据对象？
8. 在表 3.5 的文件控制参数中，哪些标记可归在上下文类数据对象中？
9. 在 IC 卡中定义了哪几种文件？对每一种 IC 卡来讲是否都是必须有的？
10. EF 文件中存放的数据有哪几种格式？
11. 文件标识符一般由几个字节组成？是否都可以用短文件标识符？

第 4 章　接触式 IC 卡的触点、电信号和传输协议

4.1　接触式 IC 卡的触点位置和功能

1. IC 卡的触点位置

ISO 7816-2 规定了 ID-1 型集成电路卡各触点的尺寸和功能。规定每个触点都应有一个不小于 2.0mm×1.7mm 的矩形表面区域，各触点间应互相隔离，但未规定触点的形状。ID-1 的尺寸为 85.6mm×53.98mm×0.76mm（宽×长×厚）。

IC 卡有 8 个触点，从 C1 到 C8，其位置在图 1.1 中给出。每个触点的功能如表 4.1 所示。

表 4.1　触点功能

触点编号	功　　能	触点编号	功　　能
C1	VCC（电源电压）	C5	GND（地）
C2	RST（复位信号）	C6	VPP（编程电压）
C3	CLK（时钟）	C7	I/O（数据）
C4	ISO/IEC JTC1/SC17 保留于将来使用	C8	ISO/IEC JTC1/SC17 保留于将来使用

2. 触点的功能

在 ISO 7816-2 中对 IC 卡的 8 个触点做出了如下规定。

- I/O：IC 卡的串行数据的输入端和输出端。
- VCC：电源电压输入端。电压容错范围为±10%。早期电压值为 5V，为了降低功耗，不断降低电压。
- GND：地（参考电压）。
- VPP：E^2PROM 的编程电压输入端。一般 IC 卡内部有升压电路，将 VCC 电压升到 E^2PROM 编程电压，VPP 触点已无用。
- CLK：时钟或定时信号输入端（由卡选用）。
- RST：复位信号（总清信号），可由读写器提供复位信号给 RST 触点；或者由 IC 卡内部的复位控制电路在加电时产生内部复位信号。RST 的作用可参阅 2.1.3 节。

剩下两个触点的用途将在相应的应用标准中规定。某些接触式 IC 卡仅有 6 个触点。

I/O 触点有如下两种可能的状态。

(1) 高状态（Z 状态）。当卡和读写器均处在接收方式时，I/O 处于 Z 状态，也可被发送方规定为 Z 状态。

(2) 低状态(A 状态)。可被发送方规定为 A 状态。

例如,卡与读写器均处于接收方式时,I/O 端处于 Z 状态。在操作期间,卡与读写器不能同时处于发送方式。

3. 接触式 IC 卡的操作过程和卡的复位

(1) 读写器和卡之间对话的顺序。

① 读写器连接卡(插卡),并“激活(Active)”IC 卡。

② 卡的复位(RST)。

③ 卡对复位的应答(Answer To RST,ATR)。

④ 在卡与读写器之间连续进行信息交换(读写器发命令,IC 卡返回响应)。

⑤ 读写器(终止 IC 卡操作)。

(2) 读写器“激活”IC 卡的操作顺序,如图 4.1 所示。

① RST 处于 L 状态。

② VCC 加电。

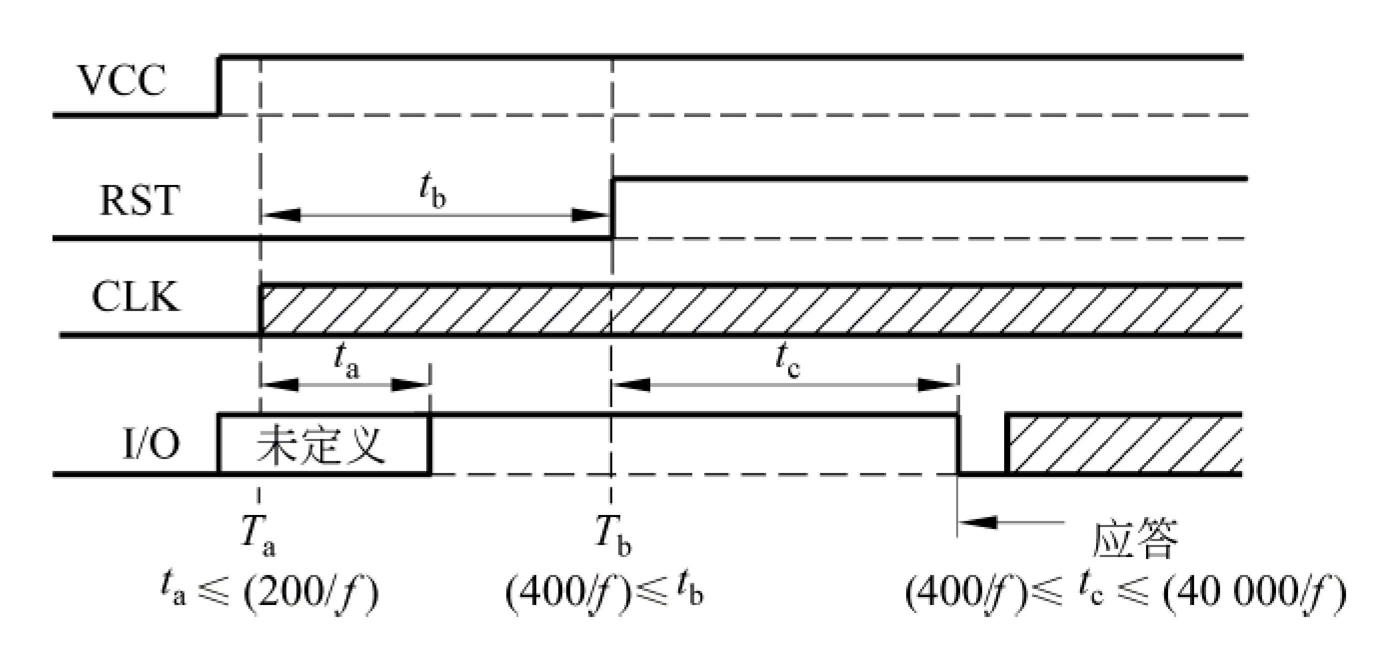


图 4.1 激活和复位

③ 读写器的 I/O 端处于接收方式。

④ 提供稳定的 CLK。

(3) IC 卡的复位。

在图 4.1 中,在 T_a 时间读写器在 CLK 端加时钟信号。I/O 端应在时钟信号加于 CLK 的 200 个时钟周期(t_a)内被卡置于状态 Z(t_a 时间在 T_a 之后)。时钟信号加于 CLK 后,保持 RST 为状态 L(低电平)至少 400 周期(t_b)(t_b 在 T_a 之后)。

在时间 T_b,读写器将 RST 置于状态 H(高电平)。I/O 上的应答由 IC 卡发出,应在 RST 信号的上升沿之后的 400～40 000 个时钟周期(t_c)内开始(t_c 在 T_b 之后)。

在 RST 处于状态 H 的情况下,如果应答信号在 40 000 个时钟周期内仍未开始,RST 上的信号将返回到状态 L,IC 卡终止操作。

4.2 异步传输的复位应答 ATR

复位应答信号以字符为单位(称为字符帧)进行传送。下面先介绍字符帧,然后描述复位应答信号。本节主要适用于智能卡(CPU 卡),逻辑加密卡在 4.3 节说明。

1. 字符帧

字符帧如图 4.2 所示。

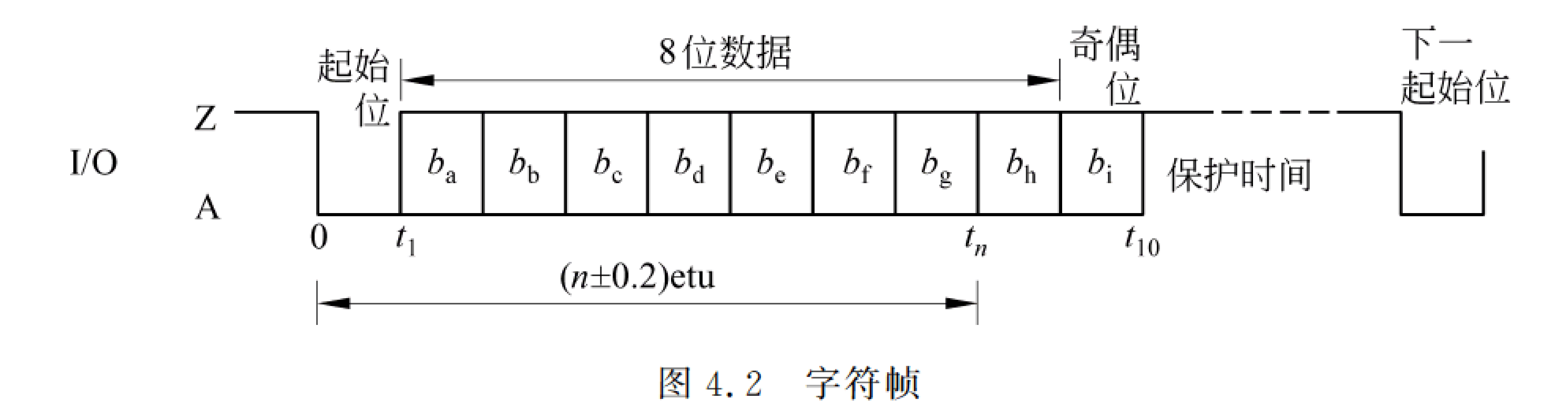


图 4.2　字符帧

在传送字符前,I/O 处于状态 Z。

每个字符由 10 位组成:起始位(1 位)为状态 A,8 位数据 b_a～b_h,第 10 位 b_i 为偶校验位(从 b_a 到 b_i,1 的个数为偶数是正确的)。每一位在 I/O 触点上的持续时间定义为基本时间单元 etu。在复位应答期间,1etu＝372 个时钟周期,即 1etu＝372/f,f 为时钟频率。

一个数据字节由 b_1～b_8 组成,b_1 为最低位,b_8 为最高位。

接收方在每一位的中间(0.5±0.2)etu 采样,采样时间应少于 0.2etu。

两个连续字符之间的延时(两起始位下降沿之间)至少为 12 个基本时间单元,包括字符宽度 10 个 etu 和一段保护时间,在保护时间内,读写器和卡都处于接收状态,因此 I/O 触点处于状态 Z。

在复位应答期间,卡发出的两个连续字符的起始位下降沿之间的延时不得超过 9600etu,这个最大值称为初始等待时间。

当奇偶校验不正确时,从起始位下降沿之后的 10.5etu 开始,收方发送状态 A 作为出错信号,该信号宽度为一个 etu 或两个 etu。发方检验 I/O 是在起始位下降沿之后的 11etu 处,若 I/O 处于状态 Z,则认为接收是正确的;若 I/O 处于状态 A,则认为有错,收方期望发方重发有错的字符或不重发。

2. 复位应答信息的内容

复位应答信息主要包括 IC 卡的发行者和应用标识符及信息传输的基本参数等。假如读写器发现问题,可立即停止操作或为后面的操作提供指示。

卡产生的复位应答信息按以下顺序传送:初始字符 TS、格式字符 T0、接口字符 TA_i TB_i TC_i TD_i(i＝1,2,…)、历史字符 T1 T2… TK(最多 15 个字符)及校验字符 TCK。其中,TS 和 T0 是一定要有的,接口字符和校验字符是可选择的。图 4.3 所示为复位应答的一般构成。在 TS 之后发送的字符数不超过 32 个。

(1) 初始字符 TS。I/O 开始处于状态 Z,然后是起始位 A,接着有两种表示方法,如图 4.4 所示。当首先传送的是字符的最高有效位时,TS 为(Z)A$\underbrace{\overset{b_a}{Z}\,\overset{b_b}{Z}\,\overset{b_c}{A}\,\overset{b_d}{A}}_{3}\,\underbrace{\overset{b_e}{A}\,\overset{b_f}{A}\,\overset{b_g}{A}\,\overset{b_h}{A}}_{F}$Z,其中 A 为逻辑电平 1,解码后的字符值为 3F,b_d、b_e、b_f 为 AAA,称为反向约定;当首

先传送的是字符的最低有效位时，TS为(Z)A b_a b_b b_c b_d b_e b_f b_g b_h
Z Z A Z Z Z A AZ，其中Z为逻辑电平1，解码后的字符值为3B，b_d、b_e、b_f 为ZZZ，称为正向约定。

（ZZAZ 对应 B，ZZAA 对应 3）

在图4.4中，可用bd、be和bf 3位来区分3F和3B。

（2）格式字符T0。字符的高半字节有效位（b_5 b_6 b_7 b_8）命名为 Y_1，当相应位为1时，分别表示后续接口字符 TA_1 TB_1 TC_1 TD_1 存在；字符的低半字节有效位（b_4 ～ b_1）命名为K，用它指出历史字符的个数0～15，如图4.5所示。

（3）接口字符 TA_i TB_i TC_i TD_i（i＝1，2，3，…）。指示协议参数。

TA_1、TB_1、TC_1、TA_2 和 TB_2 是全局性接口字符，将在后面解释。

TD_i 指明协议类型T和是否存在后续接口字符，如图4.6所示。TD_i 包括 Y_{i+1} 与T两部分。其中，Y_{i+1} 由 b_5 到 b_8 组成，分别表示后续接口字符 TA_{i+1} TB_{i+1} TC_{i+1} TD_{i+1} 是否存在，如果 TD_i 不存在，则 TA_{i+1}、TB_{i+1}、TC_{i+1} 和 TD_{i+1} 也不存在。T 由 b_1～b_4 组成，表示后续发送的协议类型。

- T＝0：异步半双工字符传输协议。
- T＝1：异步半双工分组传输协议。

在本标准中定义了 T＝0 和 T＝1 两种协议，常用的是 T＝0 协议。

- T＝2 到 T＝14：保留或其他传输协议。
- T＝15：不属于传输协议，随后的是全局接口字符。

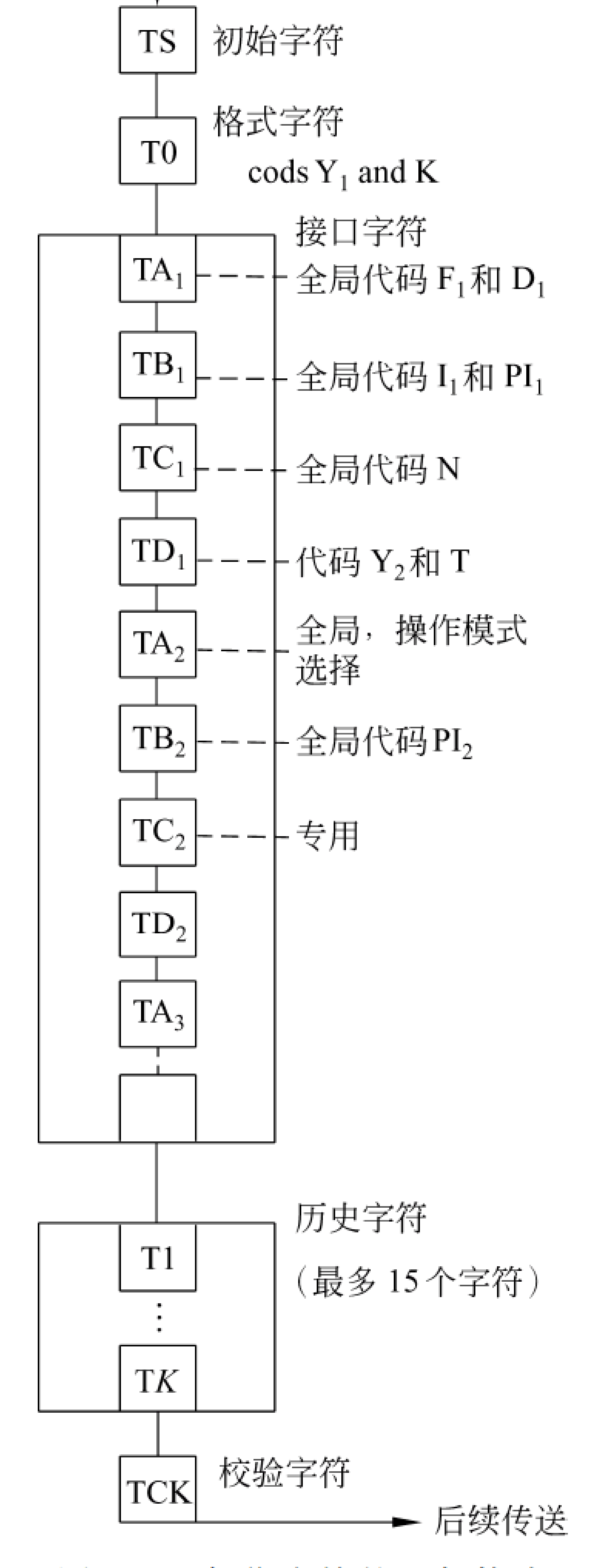


图4.3 复位应答的一般构成

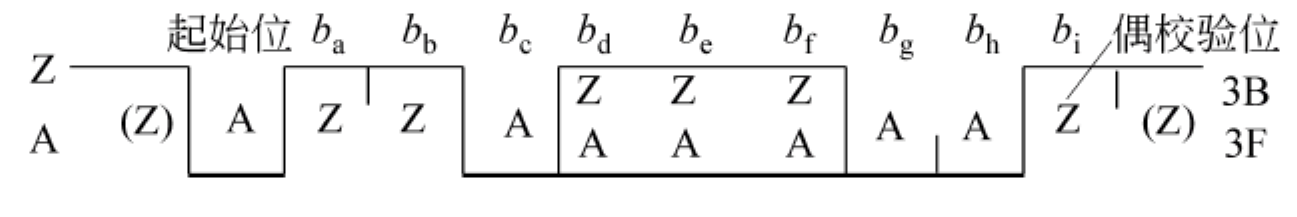


图4.4 初始字符TS

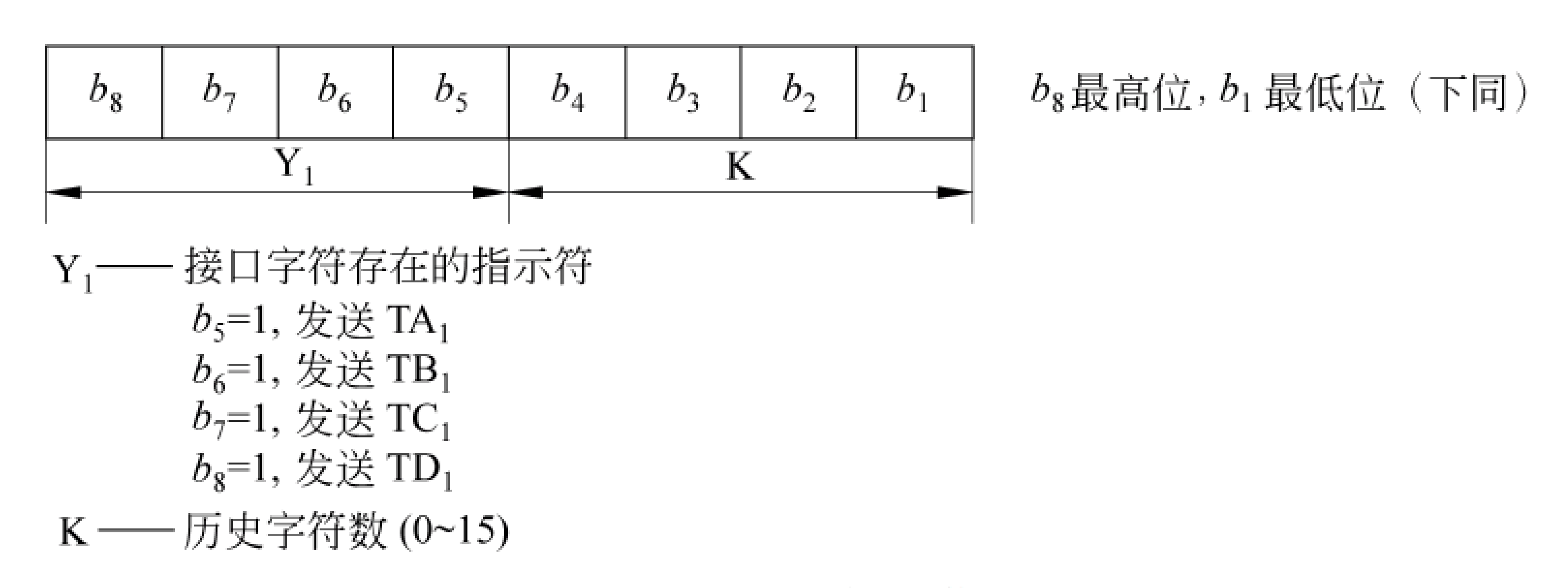


图4.5 T0提供的信息

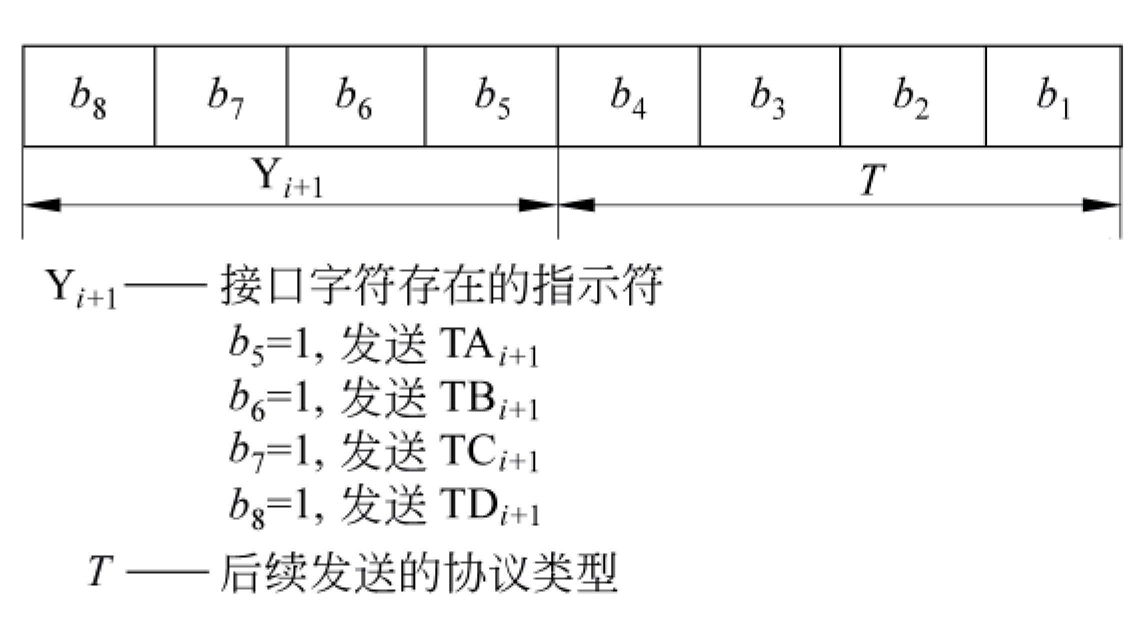


图 4.6　TD_i 提供的信息

(4) 历史字符 T1,T2,…,TK。由 T0 的低 4 位 K 指出历史字符的个数,最多不超过 15 个。

(5) 校验字符 TCK。TCK 的值应选择为使 T0 到 TCK 的所有字符的异或操作,结果为 0。如果仅用 $T=0$ 协议,将不发送 TCK,而在所有其他情况下都发送 TCK。

(6) 全局接口字符 TA_1 TB_1 TC_1 TA_2 TB_2

全局接口字符给出读写器用来计算的一些参数(F、D、N 等)。

① 参数 F、D(TA_1)。在复位应答期间的初始时钟周期将被其后传送信息的工作时钟周期所代替,F 是时钟频率转换因子,D 是位速率调整因子,用来决定工作时钟周期。

设 f 为读写器提供给 CLK 触点的时钟频率,则初始时钟周期$=\frac{372}{f}$s;工作时钟周期$=\frac{F}{D}\times\frac{1}{f}$s。初始时钟周期的 $F=372$,$D=1$。

f 的最小值为 1MHz,F 及 f 的最大值如表 4.2 所示,D 的取值如表 4.3 所示。

表中的 F1 和 D1 分别由 TA_1 的 b_8～b_5 和 b_4～b_1 给出。

如果 TA_1 不存在,则使用默认值 $F=372$,$D=1$,即工作时钟周期=初始时钟周期。

② 额外保护时间 N(TC_1)。当 N 为 0～254 时,两个字符上升沿之间的间隔$=\left(12+\left(\frac{F}{D}\times\frac{N}{f}\right)\right)$周期;当 $N=255$ 时,表示两个相邻字符的上升沿之间的间隔在 $T=0$ 时为 12etu,$T=1$ 时为 11etu,直至减至最小。N 由 TC_1 的 b_8～b_1 给出。

表 4.2　时钟频率变换因子 *F*

F1	0000	0001	0010	0011	0100	0101	0110	0111
F	372	372	558	744	1116	1488	2232	RFU
f(最大)	4	5	6	8	12	16	20	—
F1	1000	1001	1010	1011	1100	1101	1110	1111
F	RFU	512	768	1024	1536	2048	RFU	RFU
f(最大)	—	5	7.5	10	15	20	—	—

注:RFU 保留将来使用。
f 的单位为 MHz。

表 4.3　位速率调整因子 *D*

D1	0000	0001	0010	0011	0100	0101	0110	0111
D	RFU	1	2	4	8	16	32	RFU
D1	1000	1001	1010	1011	1100	1101	1110	1111
D	12	20	RFU	RFU	RFU	RFU	RFU	RFU

注：RFU 保留将来使用。

这些参数的默认值：$F=372, D=1, N=0$。

③ 参数 I_1、PI_2、PI_2（TB_1、TB_2）。指出 VPP 触点的输入电流与电压，现已无用。

④ TA_2。指出 F、D 的值是由 TA_1 还是由 PPS 决定。PPS 在历史字符之后说明。

3. 历史字符

历史字符描述卡的操作特性。复位时，卡发出的复位应答信息 ATR 中一般包含历史字符。在历史字符中用到的标记为'41'～'48'和'4F'的数据对象（见表 3.2）。

（1）国家或发行者指示符。标记为'41'和'42'，如表 4.4 所示。国家指示符由国家编码（3 个由 4 位二进制码组成的数字 0～9）和紧跟其后的数据（至少一个数字）组成，后者由相关的国家标准化组织选定（奇数个数）。发行者指示符由发行者标识号和可能紧跟其后的数据组成，如果后者存在，将由卡发行者设定。

表 4.4　国家或发行者指示符

标记	值
41	国家编码（见 ISO 3166-1）和可选的国家数据
42	发行者标识号和可选的发行者数据

注：发行者标识号可以由奇数个 0～9 的数字组成。

（2）初始访问数据。初始访问数据标记为'44'，此数据元用来指示在复位应答及可能的协议和参数选择之后的第一条命令 APDU（READ BINARY 命令或 READ RECORD 命令）。

（3）卡发行者数据。卡发行者数据标记为'45'，由卡发行者定义的数据长度、结构和编码。

（4）预先发行的数据。预先发行的数据标记为'46'，由卡制造商定义，包括卡制造商、集成电路名称、集成电路制造商、操作系统版本等的长度、结构和编码。

（5）状态信息。状态信息标记为'48'，指出历史字符中最后一个数据对象是一个字节（LCS）、两个字节（SW_1-SW_2）或 3 个字节（LCS、SW_1-SW_2）。LCS、SW_1-SW_2 的说明见 6.3.1 节。

（6）应用标识符（Application IDentifier，AID）。应用标识符标记为'4F'，此数据元指示一个应用。

应用标识符最多由 16 个字节组成，第一个字节的 b_8～b_5 用来指明分类，如表 4.5 所示。

表 4.5　应用标识符的分类

值	分　类	含　　义
'0'到'9'	—	保留
'A'	国际的	应用提供者根据 ISO/IEC 7816-5 进行国际注册
'B','C'	—	按照 ISO/IEC JTC1/SC17 要求保留供将来使用
'D'	国家的	应用提供者根据 ISO/IEC 7816-5 进行国家注册(ISO 3166-1)
'E'	标准的	对象标识符,对标准进行标识
'F'	专有的	不注册应用提供者

① 图 4.7 所示为国际 AID 的说明。它包含 5 个字节的注册应用提供者标识符(国际 RID)和专有的应用标识符扩展(Proprietary application Identifier eXtension,PIX),后者是自定义的,最多 11 个字节。

注册应用提供者标识符 (国际 RID,5 个字节,第一个字节为'AX')	专有的应用标识符扩展 (PIX,最多 11 个字节)

图 4.7　国际 AID

- 国际 RID 唯一标识应用提供者,第一个字节的 $b_8 \sim b_5$ 设置为 1010,即 'A'。之后的 9 个数字的取值为 0～9。
- 应用标识符扩展为自由编码,允许应用提供者标识不同的应用。

② 国家 AID 包含 5 个字节的注册应用提供者标识符(国家 RID)和专有的应用标识符扩展,后者是可选的,最多 11 个字节。

- 国家 RID 唯一标识应用提供者。第一个字节的 $b_8 \sim b_5$ 设置为 1101,即 'D'。之后的 3 个数字(取值为 0～9)组成国家代码(见 ISO 3166-1)。其余的 6 个数字的取值建议为 0～9。
- 应用标识符扩展为自由编码,允许应用提供者标识不同的应用。

4. 协议和参数选择 PPS

在复位应答之后,如果允许读写器向卡发送 PPS(Protocol and Parameters Selection,协议和参数选择)请求,其操作过程如下。

(1) 读写器向卡发送 PPS 请求。

(2) 若卡收到正确的 PPS 请求,则发出 PPS 确认信号来响应,否则将超出初始等待时间,卡复位。

(3) 若成功地交换 PPS 请求和 PPS 响应,这就选择好了新的协议类型和(或)传送参数,然后按规定将数据从读写器送到卡中。

(4) 若卡收到错误的 PPS 请求,则不发回 PPS 响应信号。

(5) 若初始等待时间超时,读写器将卡复位或予以拒绝。

(6) 若读写器收到错误的 PPS 响应信号,将卡复位或予以拒绝。

PPS 请求和 PPS 应答信号的组成如下。

PPS 请求和 PPS 响应信号都是由初始字符 PPSS(代码为 FF)、格式字符 PPS0,后跟 3 个任选字符 PPS1、PPS2、PPS3 及最后一个校验字符 PCK 组成的。

PPS0 的作用与接口字符 TD_i 相似,其中 b_5、b_6、b_7 分别表示任选字符 PPS1、PPS2 和 PPS3 是否存在。$b_1 \sim b_4$ 选择协议类型,b_8 留作今后使用。PPS1 给出 F 和 D 的参数值。PPS2 给出 N 值,PPS3 待定。

PCK 的值是使从 PPSS 到 PCK 的所有字符的异或结果为 0 的值。

一般情况下,如果 PPS 响应=PPS 请求,则为成功的 PPS 交换。

5. 异步半双工字符传输和分组传输协议(T=0 和 T=1)

半双工是指同一时间内,只可向一个方向传输数据,全双工是指可同时发送数据和接收数据。

1) 异步字符传输协议(T=0)

本协议以字符帧形式连续传输信息(T=0)。

本协议所用的参数都是在复位应答时所指定的,除非被协议和参数选择所修改,此时由 PPS 指定参数。

在复位应答信号 ATR 中,接口字符 $TC_2(b_8 \sim b_1)$表示出整数值 W_1。由卡发送的字符的起始位下降沿与前一个字符的起始位下降沿(由卡发送或读写器发送)之间的时间间隔不超过 $960 \times (F/f) \times W_1$,这个最大值称为工作等待时间。$W_1$ 的默认值为 10。

命令总是由读写器发向 IC 卡,IC 卡操作完成后,向读写器返回响应信息,双方传送的信息都以字符为基本单位。

在卡和读写器发送期间,字符的检错和重发如图 4.8 所示。

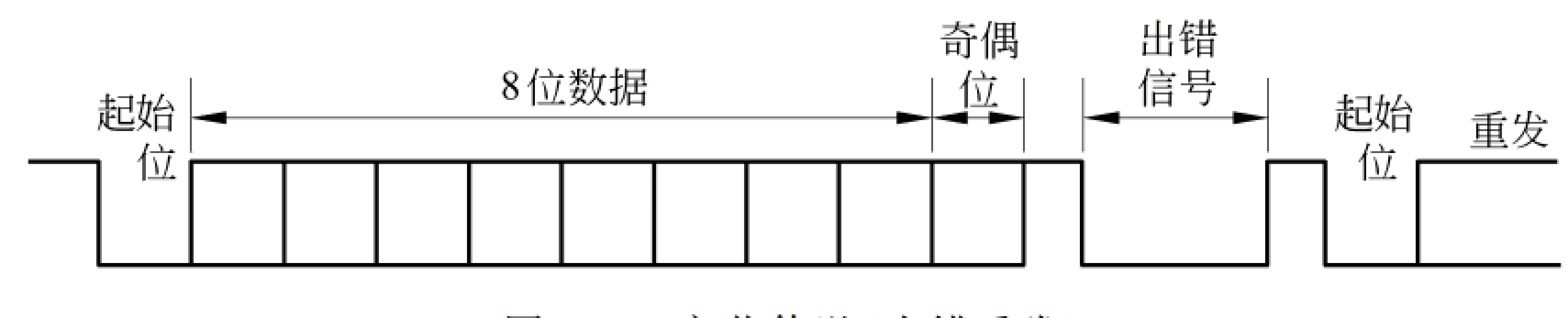


图 4.8 字节传送(出错重发)

2) 异步分组传输协议(T=1)

在复位应答 TD_1 字节中定义了 T=1,或在 PPS 中定义了 T=1 之后,将按本节讨论内容实现协议。在本节中定义了传输控制命令的结构和处理及对 IC 卡的控制。

分组传输协议的主要特点如下。

① 分组(block)是最小的数据块,它可以在 IC 卡与读写器之间传送。分组包含应用数据或控制数据(包含传输错误处理信息)。

② 为了整个分组数据的正确接收,在数据传送之前,可对分组结构的定义进行检查。

③ 无论在复位应答还是在协议类型选择 PPS 之后,都由读写器送出第一组数据来启动协议,以后可交替传送数据块。

④ 本协议使用复位应答时定义的字符帧及全局接口字节定义的物理参数。若以后被 PPS 所修改,则采用 PPS 定义的参数。

(1) 分组的基本组成——分组帧。

如图 4.9 所示，分组包括 3 个字段：开始字段(Prologue Field)、信息字段(INformation Field)和结尾字段(Epilogue Field)，其中开始字段与结尾字段是必须有的，信息字段则是可选的。

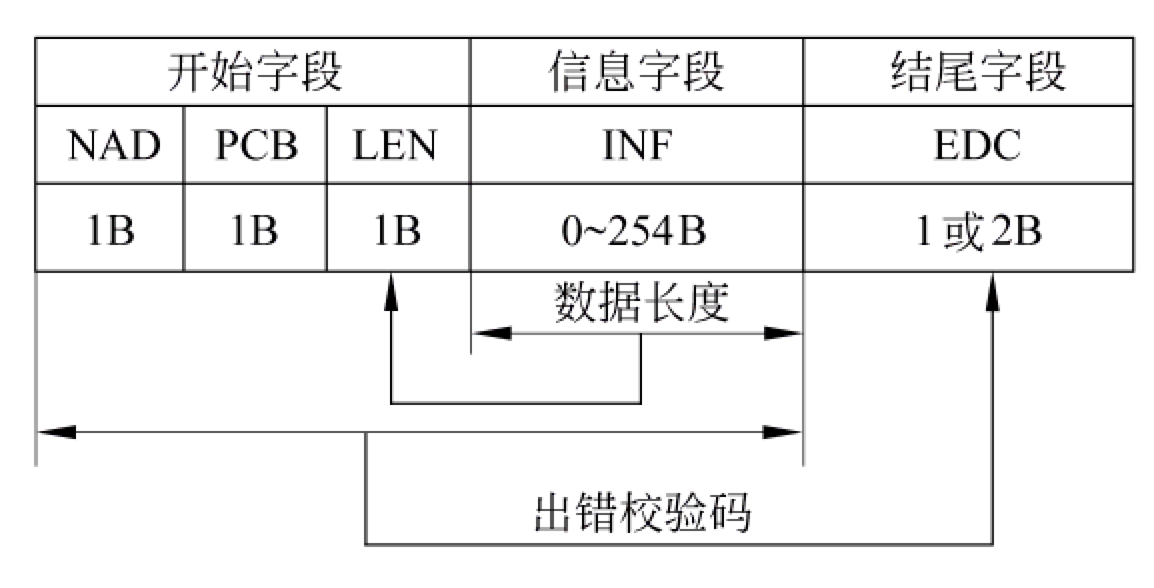


图 4.9 分组结构

① 开始字段。

• 节点地址(Node ADdress，NAD)。

$b_1 \sim b_3$ 是源节点地址(Source node ADdress，SAD)，$b_5 \sim b_7$ 是目的节点地址(Destination node ADdress，DAD)，b_4 和 b_8 最早用于 VPP 状态控制。

• 协议控制字节(Protocol Control Byte，PCB)。

协议定义如下 3 种基本分组类型。

信息分组(I-block)：用于传送信息和序列号。

接收准备分组(R-block)：用于指示是否有差错和传送序列号，它的信息字段不存在。

管理分组(S-block)：在读写器和 IC 卡之间交换控制信息，它的信息字段是否存在取决于控制功能。

• 长度 LEN(length)。

LEN 指出被传送的信息字段的字节数，其代码为'00'～'FE'(0～254B)。

② 信息字段(INformation Field，INF)。INF 字段是可选的，当它存在时，可以是应用数据(I-block)或控制和状态信息(S-block)，被传送的字节数由 LEN 指出。

③ 结尾字段。结尾字段包含被传送分组的差错校验码(Error Detection Code，EDC)，可以采用纵向冗余校验(Longitudinal Redundancy Check，LRC)(1B)或循环冗余校验(Cyclic Redundancy Check，CRC)(2B)。LRC 的值与分组中所有字节进行异或运算得结果 0，关于 CRC 的值参见 ISO/IEC 3309。

(2) 协议操作。

① 在复位应答或协议类型选择之后的第一个分组是由读写器传送到 IC 卡的，可以是信息分组或管理分组。

② 在传送一个分组(I-block、R-block 或 S-block)后，在下一个分组传送之前，发方应该接收到确认，描述如下。

信息分组内有一个发送序列号 $N(S)$，$N(S)$是一个二进制位(bit)，它的起始值为 0，在传送一个信息分组之后加 1，在 0 与 1 之间转换。

接收准备分组内有一个 $N(R)$，它的值等于下一个要传送的 I-block 中的 $N(S)$。R-block 用于链接。同时检查接收的信息是否有错(EDC 或奇偶校验错)。

管理分组有请求分组和响应分组两种，在接收到请求分组后发出一个响应分组。

③ 分组传输协议具有链接功能，当读写器或 IC 卡传送信息的长度过大时允许分组链接传输。关于“链接”的概念，在 6.1 节中有说明。

分组的链接情况受 I-block 中的协议控制字节 PCB 中的 M 位控制。M 位指出 I-block 的两种状态。

- $M=0$：表示当前的 I-block 是链接的最后一个分组。
- $M=1$：表示链接还跟有后面的分组。

④ 管理分组提出是何种请求或何种响应。

当读写器发出“重新同步请求”，此请求将分组传输协议的参数复原到初始值，IC 卡接收到重新同步请求后发出重新同步响应；“信息字段长度请求”和“信息字段长度响应”表示读写器或 IC 卡允许的最大信息长度；其他还有“中止请求”“中止响应”“等待时间的扩充请求”和“等待时间的扩充响应”等。

4.3 同步传输的电信号和复位应答

本规范(ISO/ IEC 7816-10)描述同步传输的 IC 卡(逻辑加密卡)与读写器之间的电源、信号和复位应答。

本规范说明两种类型的同步卡：第 1 类(type 1)和第 2 类(type 2)。第 2 类卡的传输率可以比第 1 类高。

1. 卡的复位

(1) 第 1 类同步卡。读写器将所有触点置于状态 L，如图 4.10 所示，然后 VCC 加电，CLK 和 RST 保留在状态 L，读写器的 I/O 触点置于接收方式。RST 至少有 50μs 维持于状态 H，然后回到状态 L。CLK 的上升沿和下降沿时间不超过 0.5μs(图 4.10 和图 4.11 中的 t_f 和 t_r)。

时钟脉冲在它与 RST 上升沿之后相隔 t_{10} 时间后给出，时钟脉冲状态 H 的持续时间为 10～50μs。在 RST 处于状态 H 时只准有一个时钟脉冲，CLK 与 RST 下降沿之间的间隔为 t_{11}。

在 I/O 触点上得到的第 1 位数据可视为应答，此时 CLK 处于状态 L，并在 RST 下降沿 t_{13} 之后有效。后续数据位在从 CLK 下降沿间隔 t_{17} 之后有效，可从其后的 CLK 上升沿采样。

(2) 第 2 类同步卡。读写器将所有触点置于的状态如图 4.11 所示，图中的 FCB 称为功能码，作用于触点 C_4 上。然后 VCC 加电，CLK、RST 和 FCB 处于状态 L，读写器的 I/O 触点置于接收模式。时钟脉冲在 VCC 上升沿之后相隔 t_{20} 后提供，时钟脉冲的持续时间为 t_{25}。在时钟脉冲上升沿之后至少相隔 t_{22} 时间 FCB 仍维持于状态 L。

在 I/O 触点上得到的第 1 位数据可视为应答，此时 CLK 处于状态 L，并在 CLK 下降沿 t_{27} 之后有效。

当 FCB 置于状态 H 时，每一个时钟脉冲上升沿可用于读出 I/O 线上的数据位。

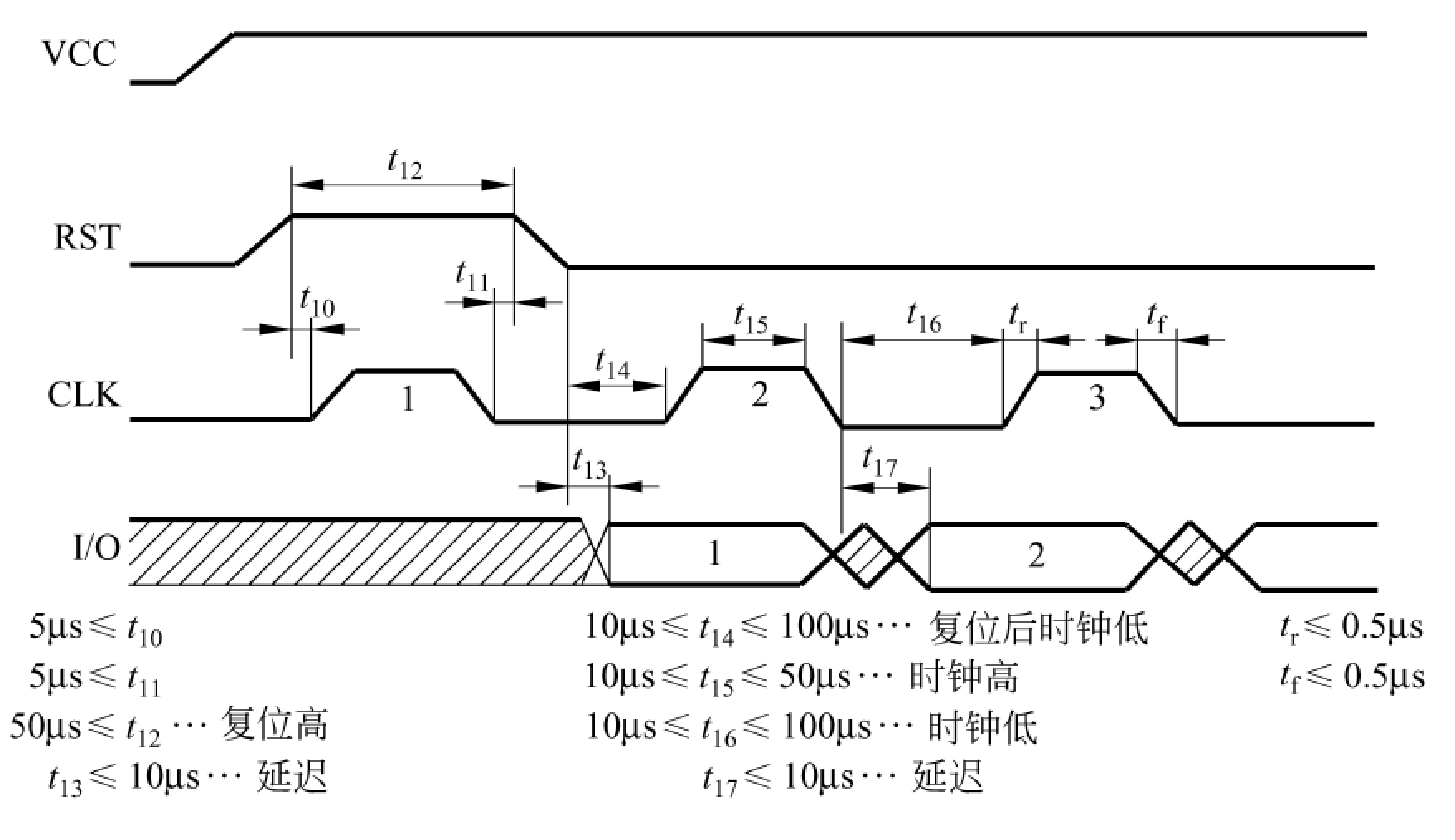


图 4.10　第 1 类同步卡的复位

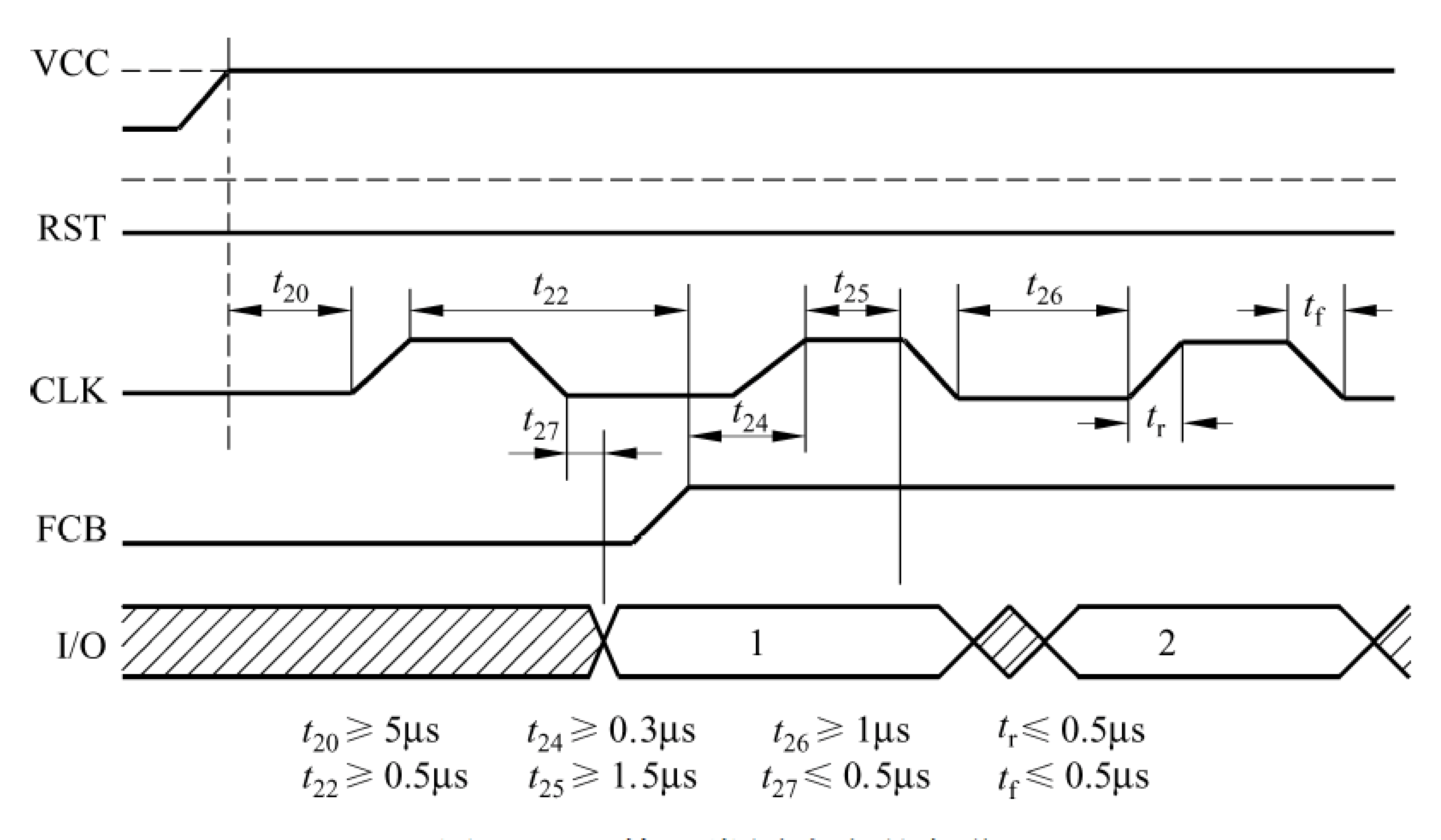


图 4.11　第 2 类同步卡的复位

2. 复位应答

在同步传输方式中，I/O 触点上一串数据位用 CLK 上的时钟信号进行同步。

(1) 时钟频率和位速率。I/O 线上的位速率与读写器发到 CLK 的时钟频率呈线性关系，如 7kHz 时钟频率相应于 7Kb/s。

最大上升沿/下降沿各为 0.5μs。

第 1 类卡：低于 50kHz 的任一频率可用。

第 2 类卡：低于 280kHz 的任一频率可用。

(2) 复位应答头的结构。复位操作的结果是从卡发送应答头到读写器。该头的长度固定为 32 位，其开始的两个字节 H1 和 H2 是必备的。

b_1～b_{32}是按时间顺序发送的信息位，最低位先发送。

(3) 复位应答头的时序。

① 第 1 类同步卡。复位之后，输出信息受时钟脉冲控制，第 1 个时钟脉冲在 RST 下

降沿之后 10～100μs(t_{14})时间内给出。时钟脉冲的状态 H 在 10～50μs(t_{15})变化,状态 L 在 10～100μs(t_{16})变化。

第 2 个及其随后的数据位在 CLK 下降沿之后 t_{17}有效,数据位依次用时钟脉冲上升沿采样。

② 第 2 类同步卡。I/O 触点的输出信息受时钟脉冲控制,第一个时钟脉冲在 FCB 上升沿之后 t_{24}时间给出。时钟脉冲状态 H 的持续时间为 t_{25},状态 L 的持续时间至少为 1μs(t_{26})。

第 2 个及其随后的数据位在时钟为低和 CLK 下降沿之后 t_{27}时间给出。数据位依次用时钟脉冲的上升沿采样。

(4) 头的数据内容。头由 4 个字节(H1～H4)组成,用于尽早决定卡与读写器是否相容,如不相容,则停止工作。

第 1 个字段 H1 是卡协议类型的编码,如表 4.6 所示。

表 4.6　H1 编码

b_8	b_7	b_6	b_5	b_4	b_3	b_2	b_1	意　　义
0	0	0	0	0	0	0	0	不用
0	×	×	×	0	0	0	0	保留给 ISO/IEC　JTC1/SC17 定义协议
×	×	×	×	×	×	×	1	由注册管理机构分配的 H1 和 H2 的编码和结构
1	1	1	1	1	1	1	1	不用
其他值								专用

第 2 个字段 H2 是 H1(协议类型编码)的编码参数,如果 H1='X0'(X=1,2,…,7),H2 的值由 ISO/IEC　JTC1/SC17 指定。

4.4　逐步被 IC 卡取代的磁卡

磁卡是一种磁记录介质卡片,曾经广泛应用于银行系统、证券系统、门禁控制系统、身份识别系统和驾驶员驾驶执照管理系统等领域。磁卡利用贴在卡上的磁条来记录持卡人的账户、姓名等信息。

4.4.1　磁道信息编码

磁卡尺寸与 IC 卡相同(ID-1 型),磁道上可以有 3 个磁道。

磁条上记录的信息具有自同步能力。编码由数据和时钟一起构成,在时钟周期(t)中间产生磁通翻转则标记为 1,而时钟周期(t)的中间没有产生磁通翻转则标记为 0,如图 4.12 所示。在时钟周期开始处都发生磁道翻转,因此具有自同步能力。

编码时,各磁道都是从右侧顶端开始编码,编码应开始于起始符第一个数据位的中心线,结束于纵向冗余校验码的最后一位(最后一位是奇偶校验位)。每个字符的位结构都

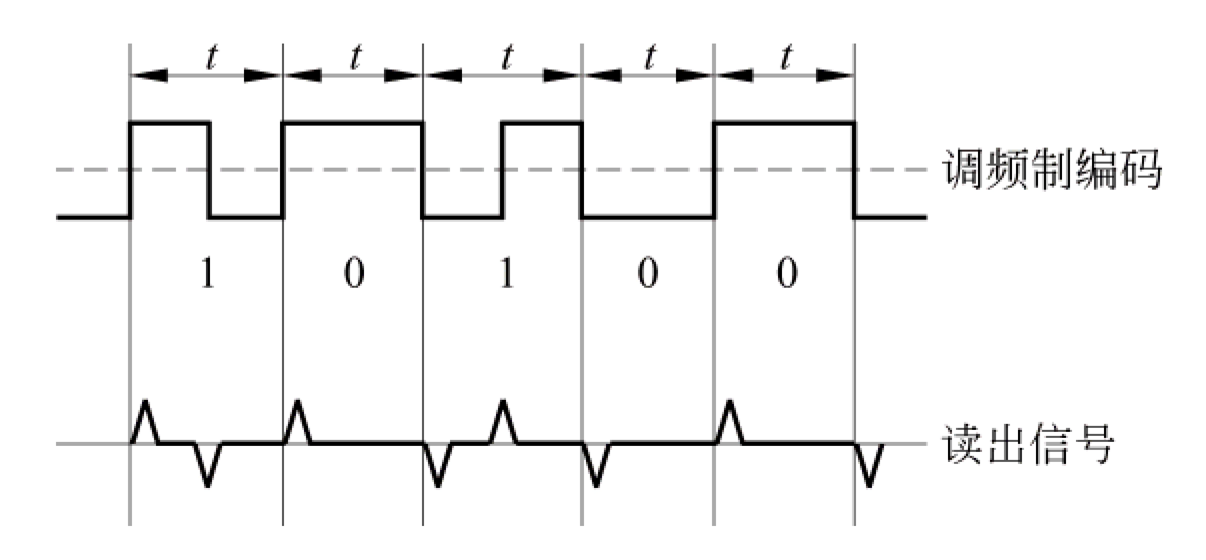


图 4.12　调频制编码和读出信号

是首先编码最低有效位(b_1)，最后编码奇偶校验位。

第一个磁道的第一个数据位之前和最后一个数据位之后的磁条空间都应该以 0 编码。

第 1 磁道采用的编码代码是字母数字型的 6 位二进制码，数字 0～9 的编码是 10～19，字母 A～Z 的编码是 21～36，并带奇校验位。磁道上包括数据字符、控制字符、起始符、结束符及纵向冗余校验字符等，全部字符数量总和不能超过 79 个。

第 2 磁道和第 3 磁道采用的编码字符集都是数字型的，其字符代码是 BCD(4 位二进制)码，并带有奇校验位。

第 2 磁道上包括数据字符、控制字符、起始符、结束符及纵向冗余校验字符等，全部字符数量总和不能超过 40 个。

第 3 磁道上包括数据字符、控制字符、起始符、结束符及纵向冗余校验字符等，全部字符数量总和不能超过 107 个。

3 条磁道都采用两种差错校验技术：奇偶校验和纵向冗余校验(Longitudinal Redundancy Check，LRC)。每一编码字符都含有一奇偶校验位。

3 条磁道的格式及内容因应用而异。后面阐述在磁卡的一个主要应用领域——金融交易卡(Financial Transaction Card，FTC)上对各磁道的格式及内容的规定。

4.4.2　金融交易卡

1. 金融交易卡的磁道记录

金融交易卡的磁道记录主要介绍金融交易卡(FTC)上的 3 个磁道的规定，这些规定也已经广泛适用于 VISA 信用卡、Master 信用卡和银联卡等。

(1) 磁道 1 的标准记录密度为 8.3bpmm±5%，每个字符的长度为 7 位(包括校验位)(bpmm 为位/毫米)。磁道 1 信息的最大长度为 79 个字母数字字符。记录格式如图 4.13 所示。

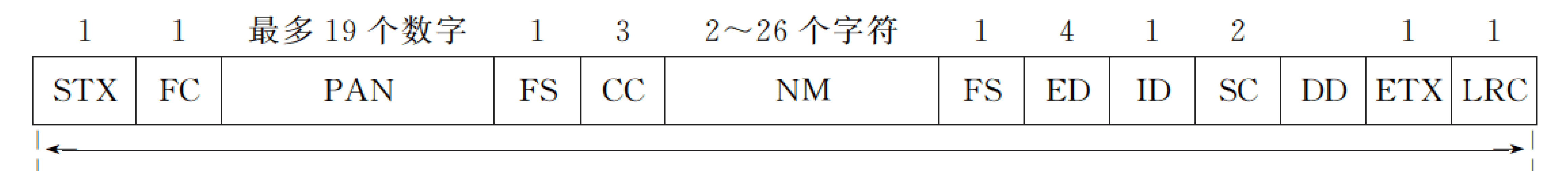


图 4.13　FTC 卡磁道 1 格式

- STX：起始字符(起始标记)。代码为 000101。
- FC：格式代码。代码为 100010。
- PAN：个人标识号码(主账号)，代表持卡人的号码，由发卡者标识号码、个人账户标识和校验数字三部分构成。
- FS：分隔符。代码为 111110。
- CC：国家代码。3 个数字，当主账号的主要行业标识符是 59(金融行业)时，这个字段按 ISO 3166 强制编码。在所有其他情形下，没有该字段。
- NM：持卡人的姓名，2～26 个字符。
- ED：失效日期。格式为 YYMM，用 4 个数字表示卡的有效期限(YY 表示年，MM 表示月)。如果不定义失效日期，该字段应为一分隔符。
- ID：交换指示符。用于国际、国内交换或用于测试。
- SC：服务代码。ID 和 SC 用来表示发卡者对持卡人提供的服务范围和类别。如果这两项内容不存在，这两个字段以一个分隔符代替。
- DD：自由数据，或称随意数据。
- ETX：结束标记(结束字符)。代码为 011111。
- LRC：纵向冗余校验字符。

(2) 磁道 2 的记录密度比磁道 1 低得多，为 3bpmm ± 3%，每个字符长度为 5 位(含校验位)，其信息最大长度为 40 个数字字符。

ISO 7813 规定了第 2 磁道的标准结构，如图 4.14 所示。

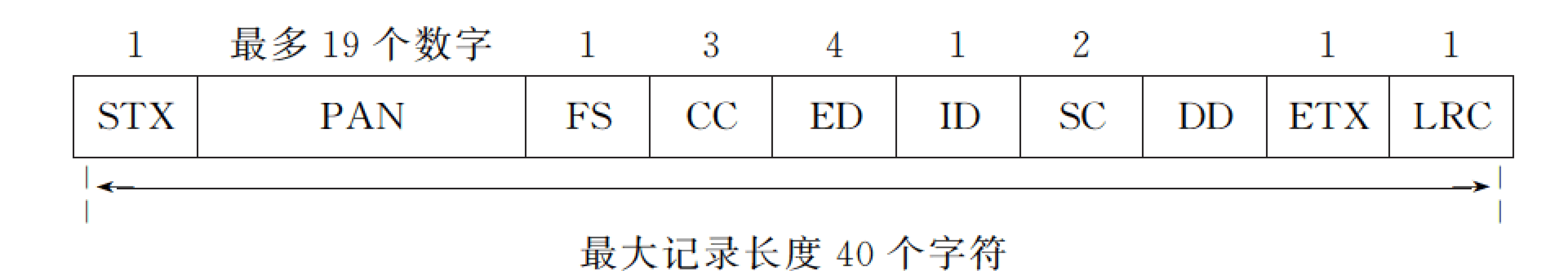


图 4.14　FTC 卡磁道 2 格式

比较第 1 磁道和第 2 磁道可以发现，两磁道的区别在于第 1 磁道比第 2 磁道多一个姓名字段，可以记录持卡人的姓名。第 1 磁道的编码字符集是字母数字的，字母主要提供给姓名字段用；第 2 磁道的编码字符集是数字的。此外，两个磁道其他字段的含义、格式及长度基本上是一样的。第 1 磁道因为信息内容多，比第 2 磁道存储密度高。实际应用时，发卡者可以根据实际需要确定选用哪条磁道，也可以将两个磁道配合起来使用，提供更丰富的信息。

(3) 第 3 磁道的记录密度为 8.3bpmm±8%，每个字符长度与第 2 磁道一样为 5 位(含校验位)，其信息最大长度为 107 个数字字符。

第 3 磁道与第 2 磁道相比，增加了一些字段，如货币类型、金额和余额、开始使用日期和有效期、输入识别码 PIN 不成功的次数。

各字段如果不需要，则以一个 FS 代替。

(4) 在金融行业，作为金融交易的磁卡，一般配合强大、可靠的计算机网络系统使用。用户的各方面信息，如金额、交易记录等，均保存在金融机构计算机的数据库中，用户所持

的卡片只是提供用户的主账号等索引信息，便于在数据库中迅速找到用户数据。

2. 各行业的主账号格式

主账号(Primary Account Number，PAN)是标识发卡者和持卡人的号码，由图4.15所示的三部分组成。

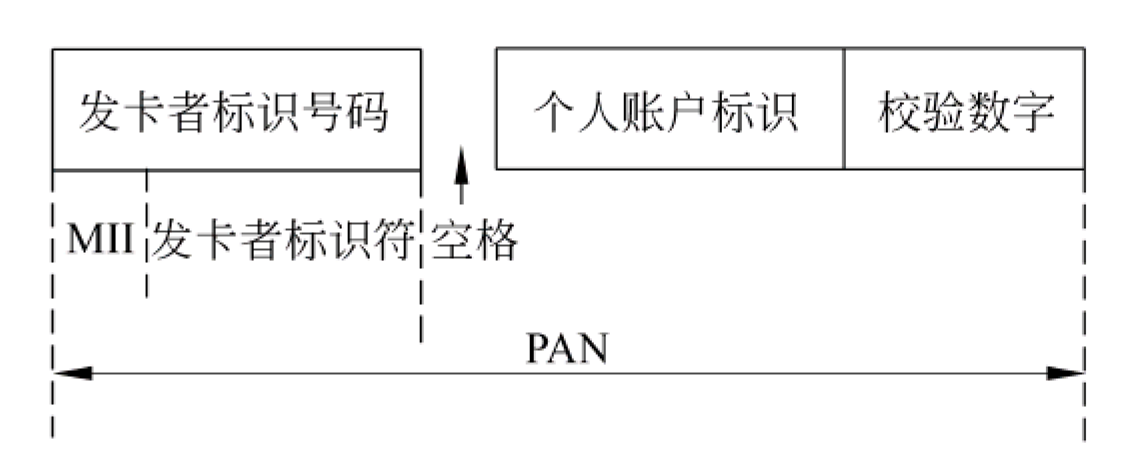


图4.15　PAN的组成

3. 发卡者标识号码

发卡者标识号码由主要行业标识符(MII)和发卡者标识符两部分组成。

MII用于标识发卡者所属行业，用一个数字表示。发卡者标识符用于标识各行业内不同发卡者，其长度由MII预先确定。例如，当MII＝1时，为航空业，发卡者标识符为3个数字；当MII＝3时，为旅游和娱乐业，发卡者标识符为5个数字；当MII＝5时，根据发卡者标识符的第1个数字确定其长度；而当MII＝5后紧跟数字9时，发卡者标识符由金融机构分配，而并非像其他情况一样由ISO注册授权机构发布，此时可将59整个看作是MII，标识金融行业。金融机构发布的发卡者标识符最多由8个数字组成，并用一个字段分隔符(空格)终止。当MII＝4或6时，也属银行/金融业。

当MII＝9时，发卡者标识符由国家代码(CCC)＋(国家标准部门分配的发卡者标识符)组成。

4. 个人账户标识

个人账户标识是由发卡部门分配给独立单位或个人的号码，用于标识一个独立的账户。

习题

1. IC卡的尺寸与磁卡是否相同？IC卡还保留磁条吗？
2. IC卡上保留有多少个触点？逻辑加密卡与智能卡的触点数是否相同？你知道每个触点的功能吗？
3. 有哪些国际标准是直接对接触式IC卡做出规定的？为什么要制定国际标准？
4. 写出IC卡激活时各触点上的电压或信号变化情况。
5. IC卡开始工作时，为什么需要由读写器送来RST信号？如果读写器不送RST信号，是否还可以采取其他办法？
6. 复位应答信号包含哪些内容？有什么作用？
7. IC卡加电后首先是由IC卡还是由读写器通知对方？
8. 复位应答后，接着是由IC卡还是由读写器发命令？执行每个命令后的响应信号是由

哪一个发出的？

9. 在异步传输协议中，$T=0$ 协议与 $T=1$ 协议的主要差别是什么？
10. 请说出字符帧的结构，当传送有错时应如何表示？
11. 在 $T=1$ 的分组传输协议中，每一个分组包括哪些字段？其中哪些字段是必须有的？哪些字段是可选的？
12. 磁卡上有几条标准磁道，采用什么编码技术？
13. 简述 FTC 卡的第 1 磁道和第 2 磁道的记录格式和内容。两者之间的主要区别在哪里？
14. 金融卡的主账号是如何构成的？其长度是多少？

第 5 章　安全和鉴别

随着计算机、互联网和通信的应用范围不断扩大，各种各样的攻击性犯罪现象已经出现，而且有增长的趋势，因此安全和保密性显得日益重要。本章重点介绍智能卡和互联网目前采用的一些安全保证措施，如身份鉴别技术、报文鉴别技术、数字签名技术，以及防火墙和防病毒技术。采用这些安全技术用以保证在开放的网络中数据传输、交换和存储的安全性。

5.1　身份认证

随着不同领域对身份认证安全程度的不同，采用了各种各样的认证方式。例如，在电子商务和金融领域往往采用“凭证＋密码”的方法，来确定客户或持卡人的身份。某些领域已引入生物特征识别技术。

5.1.1　凭证＋密码

1. 证件＋密码

例如，将金融卡插入 ATM 机，持卡人输入密码，若正确，说明持卡人是此卡的主人，允许继续操作，完成取钱、存钱或其他目的。如果输入的密码不正确，可以重新输入 3 次(或其他次数)，若每次都不正确，则将卡的功能锁住。通过指定的解锁方法后，此卡才能继续使用。其缺点是经常输入密码，可给不法分子造成偷看、窃取、监听和欺诈的机会。

2. 短信密码

服务方通过互联网接收用户的登录申请，用户方输入用户名、密码、手机号，并满足应用的条件后服务方接受登录。以后当用户提出应用请求时，服务方验证同意后向用户手机发送短信密码(随机码，一般是 6 位数字)，用户输入上述随机码后，即可进入应用服务过程。由于互联网与用户手中的手机配合工作，且随机码保留的时间很短，一次有效，从而提高了安全性。

移动互联网已开拓了移动支付的应用功能，可作为网上银行、第三方支付和电子商务交易的凭证，因此在很多场合都由电子凭证替代了纸质凭证。

3. USB Key

USB Key 是可插入计算机 USB 接口的模块。它内置单片机或智能卡芯片，可存储用户的数字证书和密码。并在 USB Key 和服务器中存放证明用户身份的密钥。当需要在网络上验证用户身份时，先由用户向服务器发出一个验证请求，然后服务器生成随机数给 USB Key。双方(服务器和 USB Key)各自通过“单向散列算法”得到运算结果，并在服务器进行比较，如果相等，则认为接到 USB 接口的 USB Key 是一个合法用户，然后可完成相应的服务。

5.1.2 生物特征识别

生物特征识别主要是通过可测量的人体或行为等生物特征进行身份认证。人体特征包含人脸、指纹、静脉、虹膜等，行为特征有签名、语音等。

生物特征识别有以下特点。

(1) 随身性。与人体绑定。

(2) 唯一性。每个人拥有不同的生物特征。

(3) 可采集性。选择的生物特征易于测量，且人们愿意接受。

1. 指纹识别

指纹是指长在人的手指指尖到第一个关节之间的表皮纹线，所有人的每一个手指指纹都不相同，具有唯一性，如果没有意外事件，可终身不变。指纹可分为左旋、右旋、螺旋、双螺旋、拱形、尖拱等类型，通过统计，前面 4 种是常见的。在此基础上再进行精细点的分析，称之为指纹的细节点。指纹的细节点包含多种类型，常用的是指纹脊线的终结点和分叉点，是一些带方向的点的集合。细节点具有稳定的特点和极高的识别率。一幅指纹图像包含约 50 个细节点。图 5.1 所示为右旋型指纹的注册过程；图 5.2 所示为脊线的终结点和分叉点，脊线是有一定密度和走向的黑式纹线，纹线之间的凹陷部分(白色)称为谷线。

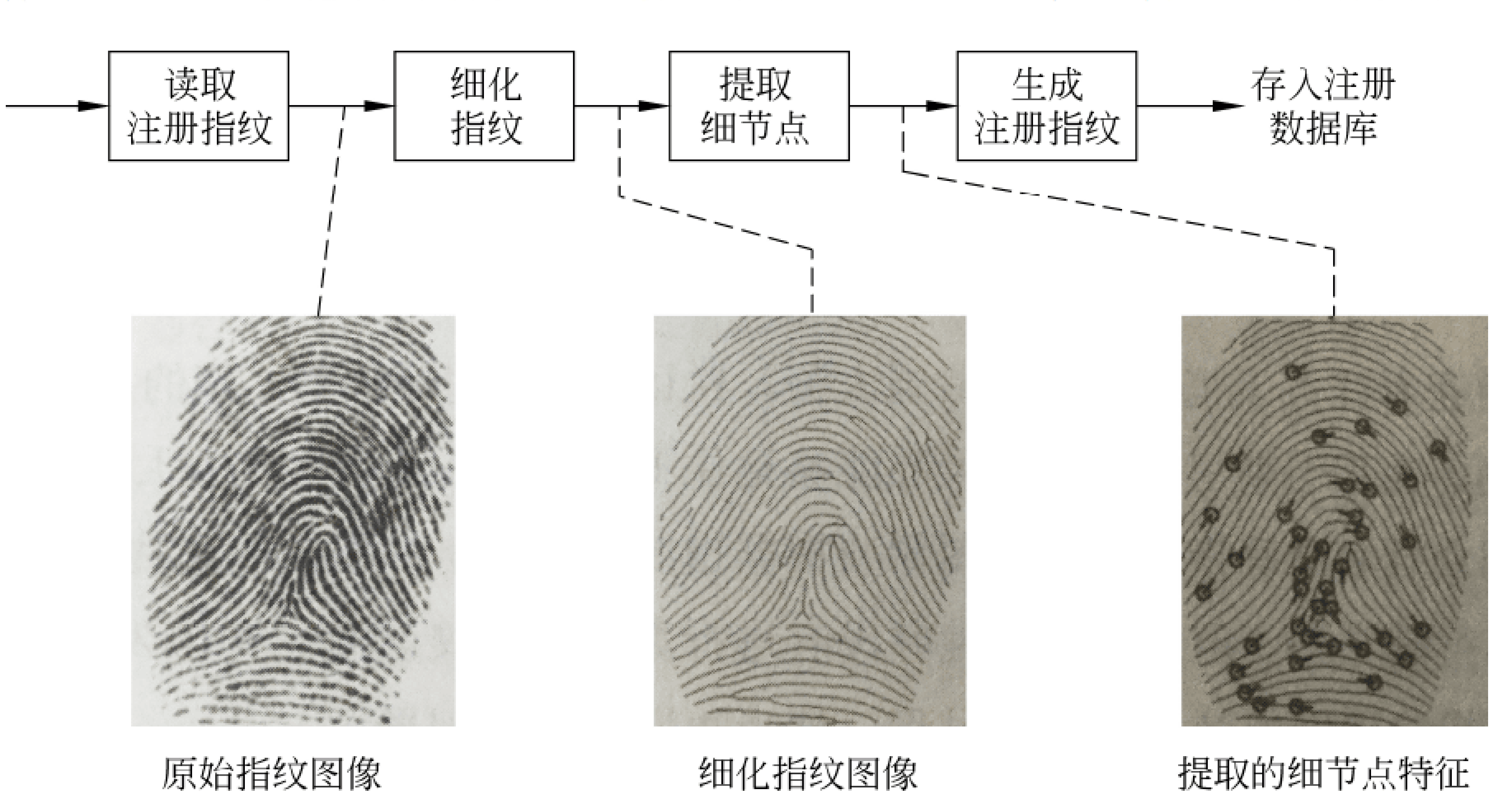


图 5.1　指纹注册过程

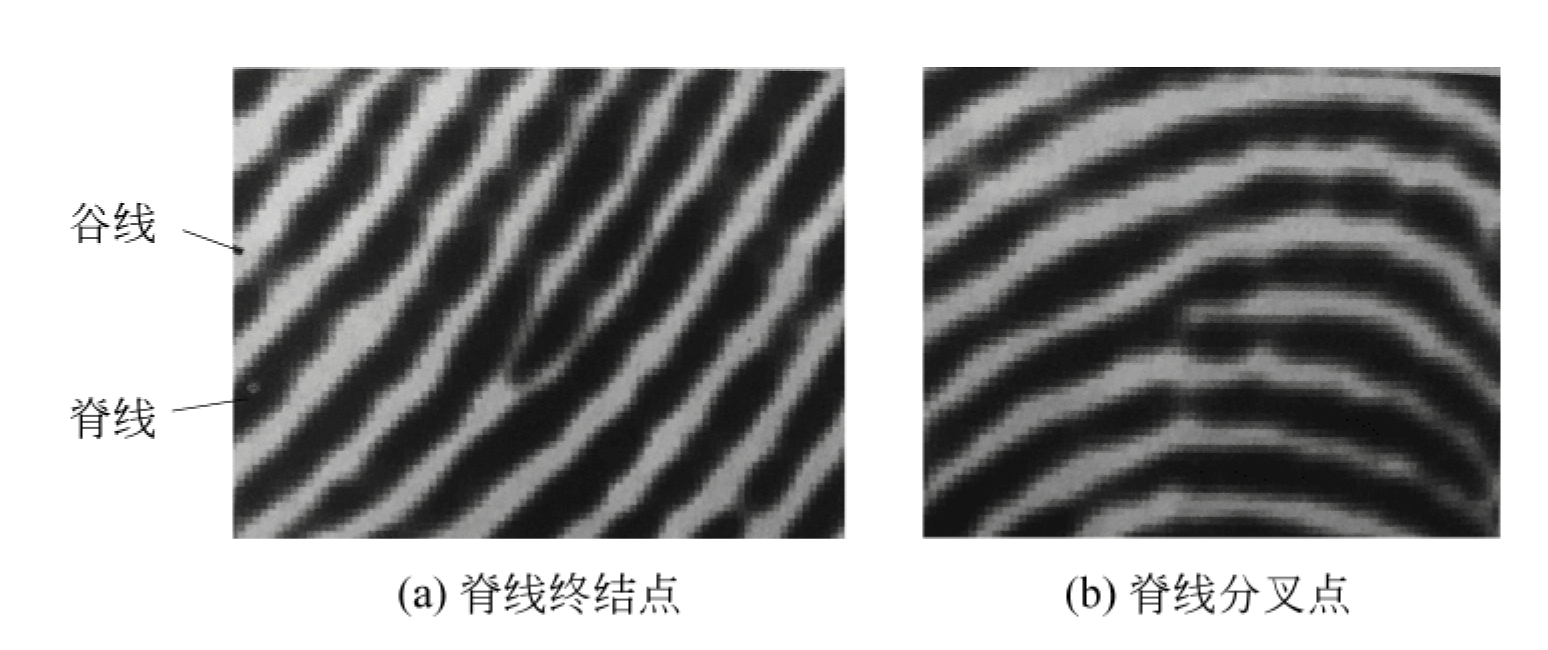


图 5.2　两类指纹细节点特征

1）指纹识别过程

（1）注册阶段。利用指纹采集仪（传感器）采集用户的指纹，转换成计算机可以处理的数字指纹图像，为了安全起见，可采集两个以上手指的指纹图像。通常采集到的指纹图像中有噪声，如果指纹采集仪认为指纹图像质量较差，可以提示用户再次输入指纹。

然后对指纹图像进行处理，得到细化的图像，从中提取细节点，生成注册指纹，存入指纹数据库。

（2）指纹识别认证。识别用户身份，现场采集用户的指纹图像进行处理（处理过程与注册阶段相同），并与注册阶段获得的指纹进行比对。

在采集用户指纹图像时，可能使用了与注册时不同类型的指纹采集仪，而且手指放置的位置有平移、旋转和形变等情况，使得两幅指纹的"细节点"不在同一坐标系中，因此需对图像进行匹配，指纹识别系统可以达到很高的识别率。图 5.3 所示为识别指纹过程。

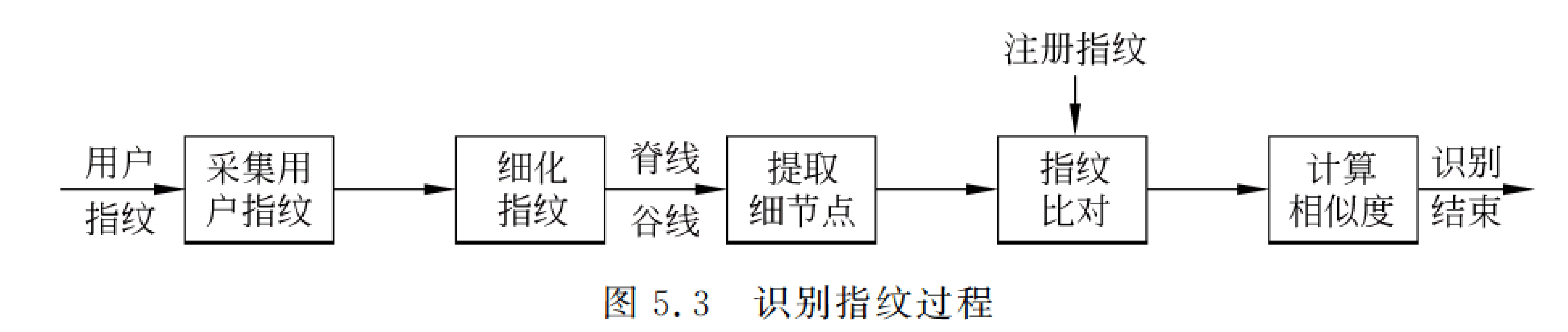


图 5.3　识别指纹过程

2）指纹图像的种类

（1）平板指纹。手指在采集仪上垂直按下再抬起，从而采集到手指中央区域的纹理信息（即纹线）。

（2）滚动指纹。手指按下后再左右滚动手指，从而采集到完整的指纹纹理信息。

（3）识别指纹。用户识别时按下的指纹。

2. 生物识别技术在社保应用

（1）指纹识别。价廉易用，应用较广泛。现场使用时，在指纹识别仪上留下指纹，要防止仿制。

（2）人脸识别。每个人的身份证上都有照片，无须另外采集和存储照片，有互联网的地方可通过计算机＋摄像头或手机终端完成自动认证。对光线和环境要求高，容易受浓妆、眼睛、表情的影响，存在双胞胎的误率、昂贵的设备费用和较慢的识别速度等缺点。

（3）声音识别（说话人识别）。无时间、地点、设备限制，但难以辨别简短的声音，识别时间比其他生物识别长，在生病时采集的声音与标本存在较大差异。

（4）静脉识别。静脉识别包括手掌、手指、手背静脉识别，一两秒即可完成，但设备较贵。

（5）虹膜、视网膜识别。通过近似红外线对眼睛扫描，虹膜是瞳孔周围的环状颜色组织，视网膜是位于眼球后部十分细小的神经。采集设备昂贵，而且需贴近设备进行扫描，

被测人接受度较低,很少使用。

3. 手写签名

手写签名作为一种身份鉴别方法已有较长的历史了。例如,签订合同、签署协议时都需要有相应负责人的签字,因为每个人签名时书写所用力度、笔迹特点等都是不一样的,根据这些特征就能够识别出签名人。手写签名识别的过程如下。

预先存储使用者真实签名样本,然后使用者通过触摸屏或手写板等输入签名到计算机,将手写签名的图像、笔顺、速度和压力等信息与真实签名样本进行比对,对所采集签名的数据信息进行预处理。合并和去除独立点和冗余点,进行平滑和倾斜校正等。接着提取特征信息,与真实签名样本进行以下对比。

(1) 签名的整体倾斜角度。

(2) 签名的宽高比。

(3) 签名笔迹长度。

(4) 签名落笔的总时间,签名提笔的总时间。

(5) 笔迹的压力变化。

(6) 笔迹形状的变化。

5.2 智能卡与互联网的通信安全与保密

智能卡必须与别的设备(或者是读写设备,或者是银行主机等)进行通信。同时,也由于智能卡自身已具备了存储及计算的能力,完全可以将它看作是一台袖珍型的计算机,因此它也在卡类系统中提供了端到端的安全控制。

一般而言,在通信方面对信息的篡改和攻击有以下方式。

(1) 对信息内容进行窃取、更改、删除、添加。

(2) 改变信息的源点或目的点,以窃取钱财。

(3) 窃取密码或推导出密码。

(4) 篡改回执。

从安全的角度考虑,就是要针对以上的这些攻击手段采取适当的技术防范措施,以求达到保证智能卡与外部设备进行信息交换过程的有效性与合法性的目的。具体而言,即是要保证该交换过程的完整性(integrity)、真实性(authenticity)、有效性(validity)和保密性(privacy)。这里,完整性是指智能卡及系统必须能检测出在它们之间交换的信息是否已经被修改了,无论这种修改是无意的还是蓄意的;有效性是指卡和系统能把真正合法的信息与一个非法人员所发的欺骗信息正确区分开,既能保证合法交易的进程,又能防止可能的诈骗行为;真实性是指智能卡和系统都必须有一种确证能力,能够确证它们各自所收到的信息都确实是真正由真实对方发出的信息,而且自己所发出的信息也确实是被真正的对方所接收到了;保密性则是指利用密码术对信息进行加密处理,从而防止攻击者窃取所交换的信息。满足这 4 种特性的要求是保证一个信息交换过程安全性的最基本条件,缺一不可。

（1）完整性的保证。为了保证所交换的信息内容不被非法修改，对之进行鉴别是非常重要的，这种鉴别称为对报文内容的鉴别。一般方法是在所交换的信息报文内加入一个报头或报尾，称其为鉴别码。这个鉴别码是通过对报文进行某种运算而得到的，它与报文的内容密切相关，报文的正确与否可以通过这个鉴别码来检验。鉴别码由报文发送方计算产生，并和报文一起经加密后提供给接收方，接收方在收到报文后，首先对之解密得到明文，然后用约定的算法计算出解密报文（明文）的鉴别码，再与收到报文中的鉴别码相比较，如果相等，则认为报文是正确的；否则就认为该报文在传输过程中已被修改过，接收方可以采取相应的措施，如拒绝接收或报警等。在鉴别过程中，鉴别算法的设计是至关重要的。最简单的算法是计算累加和，即把所传输报文中的所有位全加起来作为该报文的鉴别码。比较理想的鉴别算法一般是与密码学相联系的。鉴别过程的安全性就取决于鉴别算法的密钥管理的安全性。

（2）信息交换过程的有效性。防止对曾经发送过的或存储过的信息的再利用。例如，在某次交易过程中的一条真实信息（假设是某人从银行账户内提取了一笔钱款），如果这一消息被一个非法截听者记录了下来，他可能一遍遍地重发该消息，如果不能进行报文有效性的验证，那么该人银行账户内的存款将很快就被提光。因此，必须能保证所传送的消息每一条都是唯一的，任何随后产生的重复消息都应当被认为是非法的。实现这种报文时间性鉴别的方法有很多种，常用的方法是每条消息在发送时都附加一个发送当时的日期和时间；或者在报文中加入一个随机数等，从而保证报文的唯一性。

（3）真实性。真实性指的是对报文发送方和接收方的鉴别，即对话的双方彼此都要对对方的真实性进行验证，这种验证称为“双向鉴别”。双向鉴别的具体内容将在 5.4 节中（即在密码技术之后）讨论。

（4）保密性。保密性主要是利用密码技术对信息进行加密处理，以掩盖真实信息，使报文不可理解，达到保密的目的。由于加密、解密是通信安全中最常用的密码技术，也是通信安全的基础之一，其地位极其重要，因此下节专门进行讨论。

5.3　密码技术

密码技术的出现最初即是以通信的秘密性为目的的，其基本思想就是伪装信息，使局外人不能理解信息的真正含义，而局内人却能理解伪装信息的本来意义。密码技术的实际应用可以追溯到远古时代。公元前 50 年，古罗马的恺撒在高卢战争中就用过一种密码技术来保证其军事命令在传输过程中的保密性，他把从 A 到 W 的每个英文字母均用字母表中它后面的第 3 个位置上的字母来代替，字母 X、Y、Z 分别用 A、B、C 表示。如果分别以数字 0、1、…、25 来对应字母 A、B、…、Z，则他的这种密码变换规则就可以表示成如下形式，即

$$\Phi=\theta+3 \quad \mathrm{mod}\ 26$$

我们把被伪装的信息称为“明文”，伪装后的信息称为“密文”，而加密时所采用的信息

变换规则称为"密码算法"。在上式中，Φ 为密文字母，θ 为明文字母，3 就是这种密码算法的密钥。如果 Φ 的值超过或等于 26，则减去 26，这就是 mod 26 的意义。显然，这种密码算法是十分简单的。而到了现代，随着计算机在密码学领域的广泛应用，同时也由于现代数学的发展，使现代密码学无论在原理、概念还是工具上都有了巨大的创新与改进。然而，这些新的技术知识也给破译者提供了强有力的工具，从而又给现代密码学提出了新的任务。

所谓加密，就是对机密信息加以伪装的一个过程。被加密的信息称为"明文"，而把密文转变为明文的过程称为"解密"。以下形式表明了这个过程。

明文 P → 加密 $E(P)$ → 密文 C → 解密 $D(C)$ → 原明文 P

明文用 P 表示，在智能卡中，它表现为比特流或二进制数据。

密文用 C 表示，它也是二进制数据，加密函数 E 作用于明文 P 得到密文 C，其表达式为

$$E(P)=C$$

解密函数 D 作用于 C 产生明文 P，其表达式为

$$D(C)=P$$

由于对明文先加密，再解密将恢复出原来的明文，因此下面的等式成立，即

$$D(E(P))=P$$

现代的加密算法都使用密钥，用 k 表示，则下述加密/解密表达式成立，即

$$E_k(P)=C$$

$$D_k(C)=P$$

$$D_k(E_k(P))=P$$

在本书中，算法（algorithm）指的是加密和解密时所用的数学变换，密码体制（cryptosystem）指的是算法和实现它的方法。

一个密码体制一般由两个基本要素构成：密码算法和密钥。这里，密码算法是一些公式、法则或程序，一般与现代数学中的某些理论相联系。考虑到密码算法本身很难做到绝对保密，因此现代密码学总是假定密码算法是公开的，真正需要保密的是密钥，即一切秘密都隐藏在密钥中。所以，现代密码学中密钥管理是极为重要的一个方面。

与加密对应的是密码分析，也称"破译"，是指非授权者通过各种方法窃取密文，并通过各种方法推导出密钥，从而读懂密文的操作过程。而用以衡量一个加密系统的不可破译性的尺度称为"保密强度"。一般而言，一个加密系统的保密强度应该与这个系统的应用目的、保密时效要求及当前的破译水平相适应。能够达到理论上不可破译是最好的（非常难），否则也要求能达到实际的不可破译性，即原则上虽然能够破译，但为了由密文得到明文或密钥必须付出十分巨大的计算代价，而不能在希望的时间内或实际可能的经济条件下求出准确答案。

密码体制的分类很多。例如，可以按照密码算法对明文信息的加密方式，分为序列密

码体制和分组密码体制；按照加密过程中是否注入了客观随机因素，分为确定型密码体制和概率型密码体制；按照是否能进行可逆的加密变换，分为单向函数密码体制和双向函数密码体制。卡内常用的是按照密码算法所使用的加密密钥和解密密钥是否相同，能不能由加密过程推导出解密过程（或者反之，由解密过程推导出加密过程），而将密码体制分为对称密码体制和非对称密码体制，在下面将予以讨论，并简述属于单向密码体制的 Hash 算法。在某些卡内还使用了其他算法，如手机的 SIM 卡采用 A3、A5 和 A8 加密算法，Philips 公司支持 CRYPTO 1 流密码加密算法。

5.3.1 对称密码体制

对称密码体制又称为单钥密码体制、对称密钥密码体制、秘密密钥密码体制。在这种密码体制中，加密密钥和解密密钥是相同的，即使二者不同，也能够由其中的一个很容易地推导出另一个。因此它的密钥必须极为安全地传递和保护，从而使密钥管理成为影响系统安全的关键性因素。

目前，在智能卡中应用较多的是对称密码体制，其中较典型的加密算法是 DES 算法。该算法是一种分组密码算法，分组密码算法的基本设计技巧是 Shannon 所建议的扩散(diffusion)和混乱(confusion)。扩散就是要将每一位明文尽可能迅速地作用到较多的输出密文位中，以隐蔽明文的统计特性。扩散同时也是指把每一位密钥的影响尽可能地扩散到较多的输出密文位中。混乱是指密文和明文之间的关系应该尽可能的复杂化，要避免出现很有规律的、线性的相关关系。同时不能让多个明文对应同一密文状态，使解密出现困难。

DES 是 IBM 公司于 1975 年研发成功并公开发表的，这也开创了公开全部算法的先例。

1. DES 算法的加密过程

DES 算法是把 64 位的明文输入块变换为 64 位的密文输出块，它所使用的密钥也是 64 位，其中 8 位为奇偶校验位。整个算法的流程如图 5.4 所示。要加密的一组数据先经过初始置换 IP 的处理，然后通过一系列迭代运算，最后经过 IP 的逆置换 IP^{-1} 给出加密的结果。图 5.4 中，k_i ($i=1\sim16$) 是初始密钥 K 经分解、移位后产生的 16 个 48 位长的子密钥。从图中可见，与密钥有关的算法包括子密钥的生成和密码函数 f。

1) 初始置换 IP

首先讨论初始置换 IP。IP 的功能是将输入的 64 位数据块按位重新组合，并把输出分为 L_0 和 R_0 两部分，每部分各长 32 位。重新组合的规则如表 5.1 所示。

表 5.1 初始置换 IP

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

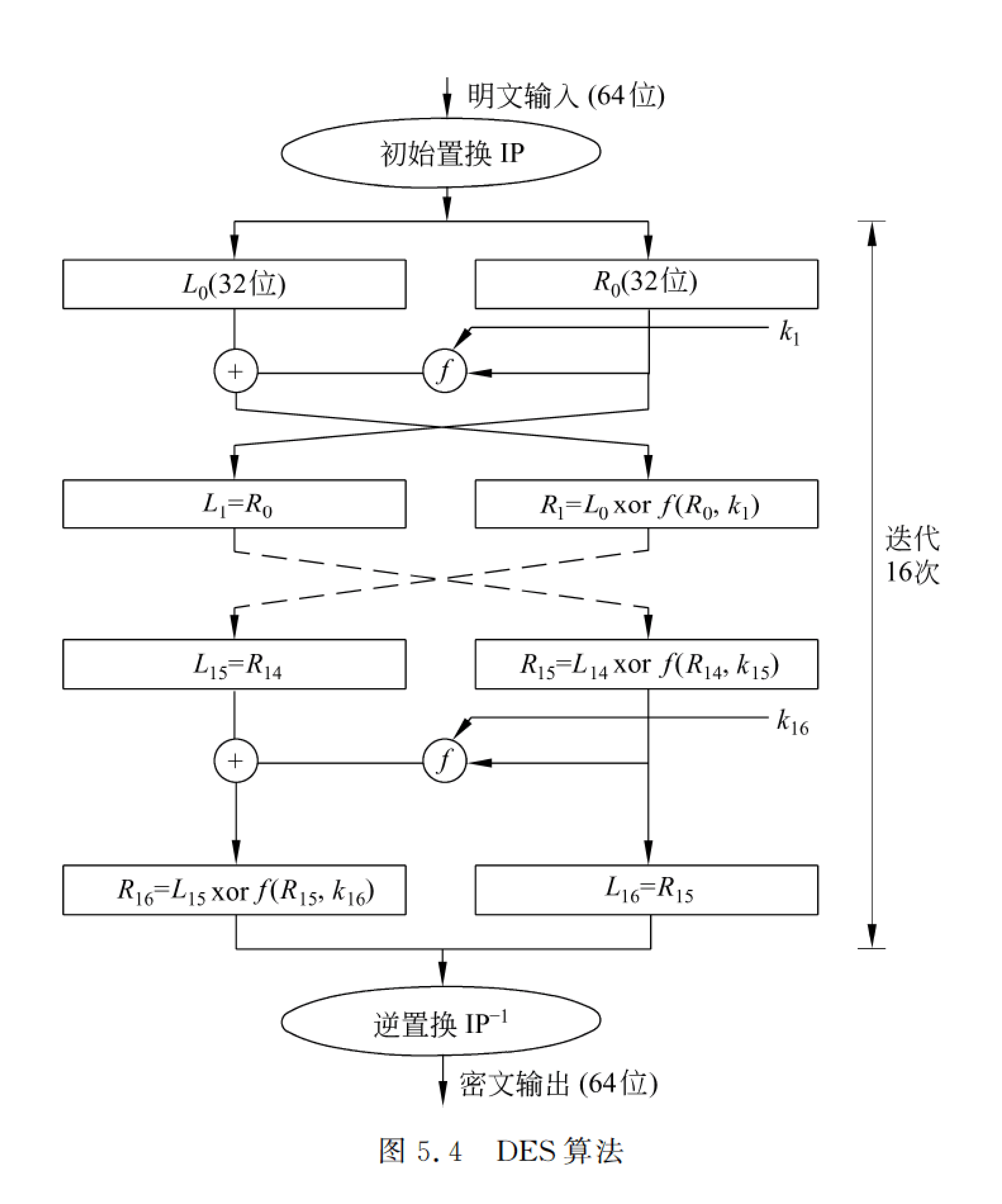


图 5.4　DES 算法

即将输入的第 58 位换至第 1 位，第 50 位换至第 2 位，第 1 位换到第 40 位，依次类推，最后一位是原来的第 7 位。L_0 和 R_0 则是换位输出后划分的两部分，L_0 是输出结果的左边 32 位，R_0 就是右边的 32 位。即如果令置换前的输入值为 $b_1b_2\cdots b_{64}$，则经过初始置换后的结果为

$$L_0=b_{58}b_{50}\cdots b_8 \quad R_0=b_{57}b_{49}\cdots b_7$$

2）16 次迭代

接下来就是迭代过程，将 R_0 进行扩展，并与子密钥 k_1 进行运算得到 $f(R_0,k_1)$，再与 L_0 按位模 2 加得到 R_1，将 R_0 作为 L_1，就完成了第一次迭代，依次类推，第 i 次的迭代可以表示为

$$L_i=R_{i-1}$$
$$R_i=L_{i-1} \text{ xor } f(R_{i-1},k_i)$$

式中，xor(异或)为按位作模 2 加。

在迭代过程中，f 的操作过程是：首先将 32 位的 R_{i-1} 扩展至 48 位，与子密钥 k_i 按位模 2 加后，再进行两次置换，得到 32 位输出 $f(R_{i-1},R_i)$。

3）逆置换 IP^{-1}

经过 16 次迭代运算后，得到 $R_{16}L_{16}$，将之作为输入，进行逆置换 IP^{-1}，即得到密文。

IP^{-1}完成的功能正好是 IP 的逆过程。

上述的各次置换都可从 DES 算法的列表中查到，但无法用公式表示，达到扩散和混乱的目的。

4）子密钥 $k_1 \cdots k_{16}$ 的生成

下面介绍子密钥的生成。子密钥 k_i 的生成过程如图 5.5 所示。

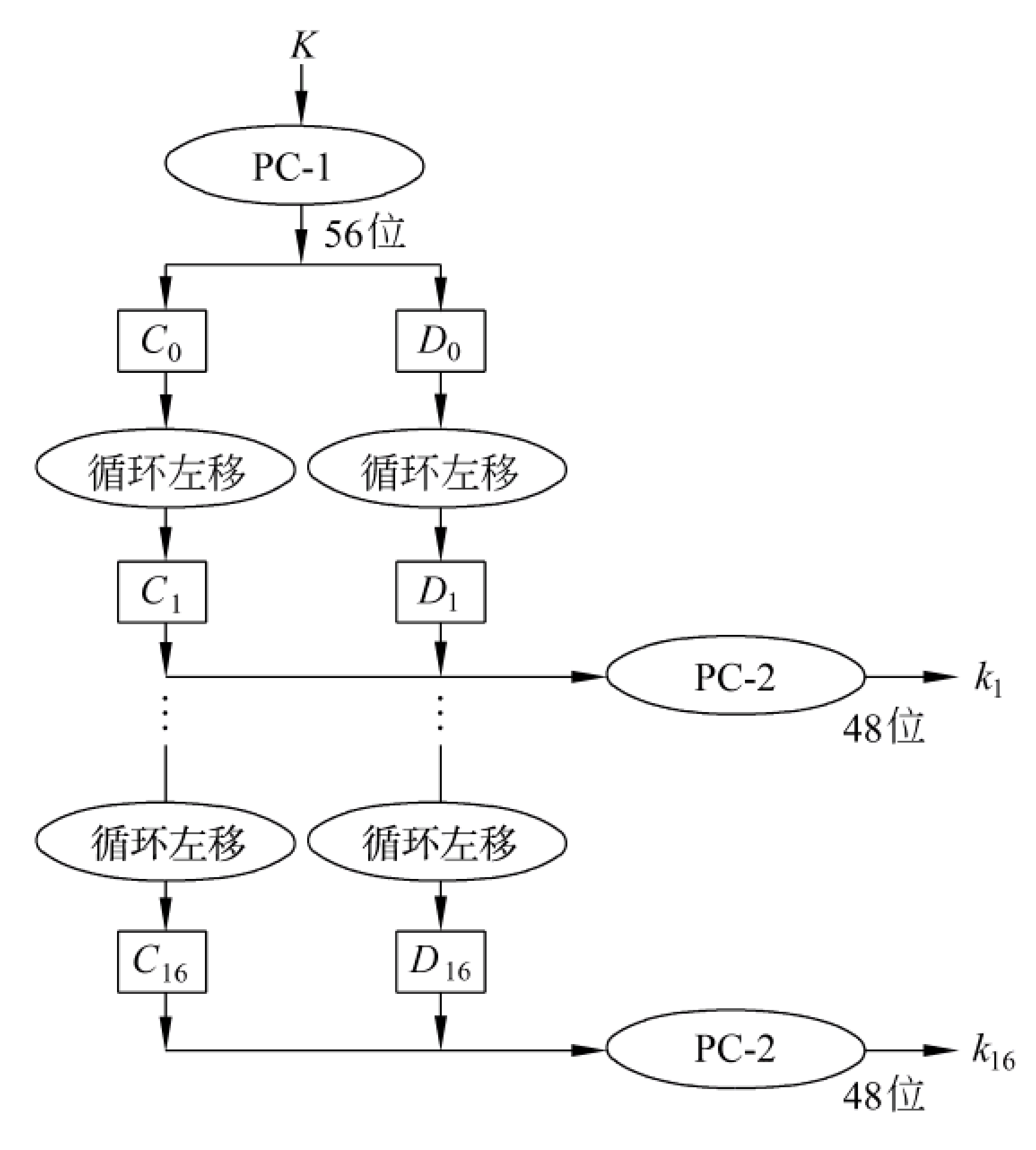


图 5.5　子密钥的生成

密钥 K 本身为 64 位，但其中第 8、16、24、…、64 位是奇偶校验位，所以 K 实际只有 56 位。将这 56 位的数据经过选择换位 PC-1 后产生的结果分为两部分：C_0 和 D_0 分别是左、右各 28 位，然后分别经过循环左移位，得到 C_1、D_1，合并后，再经缩小换位 PC-2，即得到 48 位的子密钥 k_1。同样，将 C_1、D_1 经过循环左移，合并后，再经缩小换位 PC-2，得到子密钥 k_2，依次类推，可以产生 k_3，k_4，…，k_{16}。

以上介绍了 DES 的加密过程。文中提到的换位、置换都有表可查，在本书中基本上都省略了。

DES 的解密算法是一样的，只是采取逆向处理。例如，在第一次迭代时使用 k_{16}，第二次使用 k_{15}……最后一次使用 k_1。

2. DES 算法的安全性

DES 算法的优点是加密/解密的速度快（运算简单），适用于对大量数据进行加密的场合。

DES 算法的安全性在于攻击者破译的方法除了穷举搜索外还没有更有效的手段，而搜索 56 位长的密钥的穷举空间是 2^{56}，在早期，如果用一台计算机搜索，就需要若干年的时间。随着科学技术的发展，更高速计算机、分布式计算机和网络的出现，会使 DES 的安全性受到威胁，某些部门已明确表示不再使用 DES 算法，但目前 DES 算法还是广泛应用于智能卡系统中。例如，在国际和国内流行的金融卡中主要采用 DES 算法，但为了安全

起见，采用双长度密钥的 3-DES 算法。

3. 三重 DES(3DES)

三重 DES 用 3 个密钥对明文加密/解密 3 次。发送者先用第 1 个密钥对明文加密，然后用第 2 个密钥解密，最后用第 3 个密钥加密；接收者用第 3 个密钥解密，用第 2 个密钥加密，最后用第 1 个密钥解密。

$$C=E_{k3}(D_{k2}(E_{k1}(P)))$$

$$P=D_{k1}(E_{k2}(D_{k3}(C)))$$

图 5.6 所示为三重 DES 算法的加密/解密过程，密钥的长度为 168 位(3×56 位)。如果 $k_3=k_1$，则用两个密钥，密钥的长度为 112 位。一般使用的密钥长度为 112 位。

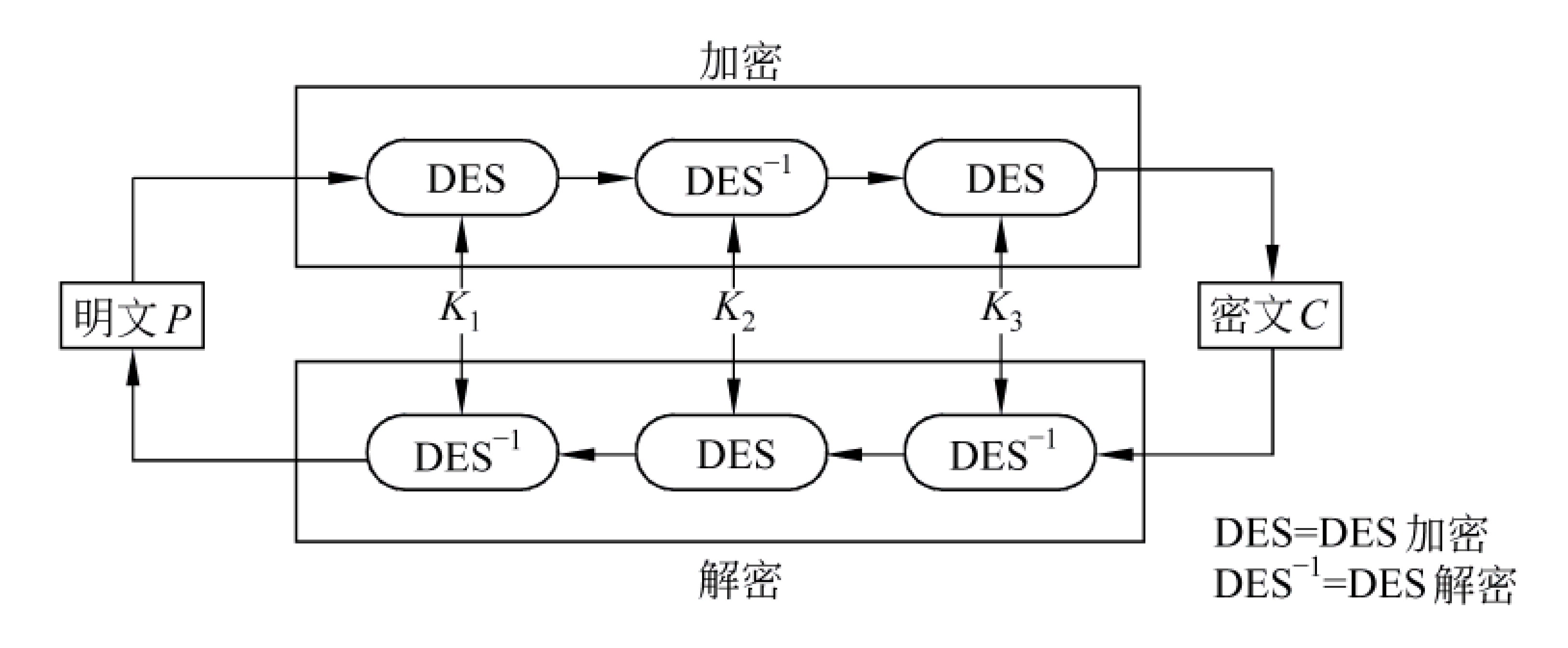


图 5.6　三重 DES

其后发展的高级加密标准 AES(Advance Encryption Standard)是美国国家标准技术研究所 NIST 旨在 21 世纪取代 3DES 的加密标准，加密数据块分组长度为 128 位，密钥长度为 128 位、192 位或 256 位。

对称密码体制的密钥使用了一段时间以后就需要更换，加密方需通过某种秘密渠道把新密钥传送给解密方。在传递过程中，密钥容易泄露。

由于对称密码体制的加密密钥和解密密钥是相同的，在智能卡中采用 DES 算法，当信息的收发方对信息内容及确定有错方产生争执时，DES 算法就显得无能为力了。典型的例子是发送方可能是不诚实的，由于他发送的信息可能对他不利而抵赖，接收方又无法证明该消息确实是由发送方发过来的。在这一争执中，作为仲裁的第三方也无法区分哪一方有错，而使用非对称密码体制可以消除这种争执。

5.3.2　非对称密码体制

非对称密码体制又称为双钥密码体制或公开密码密钥体制。在这种密码体制中，加密和解密分别通过两个不同的密钥实现，并且由其中的一个密钥推导出另一个密钥是很困难的。采用非对称密码体制的每个用户都有一对由认证机构(Certification Authority，CA)发放的数字证书和一对密钥，其中一个可以公开，称为公开密钥，简称为公钥；另一个发给用户秘密保存，称为私钥。有关 CA 的概念和作用参见 5.3.4 节。

非对称密码体制具有如下的一些优点。

(1) 密钥分发简单。由于加密和解密密钥不同，而且不能从加密密钥推导出解密密钥，因而加密密钥表可以像电话号码本一样分发。

(2) 秘密保存的密钥量减少。每张智能卡只需秘密保存自己的解密密钥。

(3) 公钥的出现使得非对称密码体制可以适应开放性的使用环境。

(4) 可以实现数字签名。

数字签名主要是为了保证接收方能够对公正的第三方(仲裁方)证明其收到的报文的真实性和发送源的真实性而采取的一种安全措施,可以保证收发方不能根据自己的利益来否认或伪造报文。

但是,目前非对称密码体制也存在一些问题需要解决。由于非对称密码体制不仅算法是公开的,而且公开了公钥,从而就提供了更多的信息可以对算法进行攻击。此外,至今为止,所发明的非对称密码算法都是很容易用数学公式来描述的,因此它们的保密强度总是建立在对某一个特定数学问题求解的困难性上。然而,随着数学研究的发展,许多现在看起来难以解决的数学问题可能在不久的将来会得到解决,这也是非对称密码体制目前的一个不足之处。另外,非对称密码体制加密/解密的计算时间长,因此对 IC 卡中的微处理器性能要求较高,或者配置数据处理单元,这也影响它的推广使用。尽管如此,由于非对称密码体制的优点还是很明显的,而且在某些特殊的场合也不得不使用非对称密码体制,因此对非对称密码体制的研究一直在进行中,其中最为著名的一个例子就是 RSA 算法。

RSA 算法是由 Rivest、Shamir 和 Adleman 3 个人提出来的,从提出到现在已经经受了各种攻击的考验,被认为是目前最优秀的非对称密码方案之一,国外也已经研制出了多种 RSA 专用芯片。下面对 RSA 算法本身加以简单介绍。

RSA 算法也是一种分组密码算法,它以数论为基础,其安全性是建立在大整数的素数因子分解的困难性上的,后者在数学上至今还没有一种有效的简便算法。要建立一个 RSA 密码系统,首先任意选取两个大素数 p、q,计算乘积 n,即

$$n = p \cdot q$$

并得到 Euler 函数,即

$$\varphi(n) = (p-1)(q-1)$$

然后,任意选择一个与 $\varphi(n)$互素的整数 e 作为加密密钥,再根据 e 求出解密密钥 d,d 满足

$$de \equiv 1 \bmod \varphi(n)$$

事实上,加密密钥 e 和解密密钥 d 在功能上是完全可以互换的,因此在生成 e、d 时,不论先假设哪一个,再由它去求另一个都是可以的。在这些参数(p、q、n、$\varphi(n)$、e、d)中,p、q、$\varphi(n)$、d 是保密的,n、e 则是公开的。在后面的计算中,p 和 q 已不再需要,可以舍弃,但绝不能泄露。有了这些参数,就能进行加密和解密运算了。

加密之前,先将明文(以 m 表示)数字化,把用二进制数据表示的明文分成长度小于 $\log n$ 位的明文块,以确保每个明文块值不超过 n。对明文 m 加密的过程是

$$c \equiv E(m) = m^e \bmod n$$

式中,c 为密文。

解密过程则是

$$m \equiv D(c) = c^d \bmod n$$

利用 Euler 定理可以证明该加密/解密过程的一致性，具体的证明过程在这里不再论述。

至于 RSA 算法的安全性，由于无法从理论上直接把握它的保密性能，因此目前的结论仅仅是：攻破 RSA 算法不会比大数分解问题更难。RSA 的成功刺激了大数分解技术的改进，使各种新技巧不断出现，今后是否会有突破性进展还难以预料，因此当准备采用 RSA 时，应当考虑上述情况。

RSA 算法的主要缺点是：密钥的产生过于麻烦，要受到素数生成技术的限制；而且为了保证安全性，其密钥要求在 500 位以上，从而使运算时间增加。

数字签名过程如下。通信双方各有一对密钥(公钥和私钥)，假设发送方 A 的加密算法为 E_A，解密算法为 D_A。接收方 B 的加密算法为 E_B，解密算法是 D_B。若 A 要向 B 送去信息 m，则 A 先用自己的私钥对 m 进行加密，再用 B 的公钥进行解密得 C。

$$C=D_B(E_A(m))$$

B 收到密文后，先用自己的私钥对 C 进行加密。

$$E_B(C)=E_B(D_B(E_A(m)))=E_A(m)$$

再用 A 的公钥对 $E_A(m)$ 进行解密，则得

$$D_A(E_A(m))=m$$

从而得到了明文 m。如果产生问题，由于 C 用了 A 的私钥才能产生，因此 A 不能推卸责任，从而达到签名的目的。

数字签名的实现方法不是唯一的。例如，认证机构 CA 的签名使用 Hash 算法。

智能卡微处理器的计算能力还不强，如果用程序实现 RSA 算法，将使智能卡的响应时间慢得令人无法忍受。因此，通常在卡内设置有适用于加密/解密运算的协处理器。

5.3.3 单向密码体制

Hash 算法(或称为散列函数)归属单向密码体制，只能实现加密过程，无解密功能，从任意“大长度”的信息(明文)产生固定“长度”的摘要信息(又称为哈希值)。

Hash 一般翻译成散列或直接音译为哈希。所以 Hash、散列、哈希成为同义词。哈希算法的主要目的是认证传输的信息无差错或不被篡改。

哈希算法的实现措施如下。

1. 在存储器中建立哈希表(或称为散列表)

表内存放的是从原信息生成的摘要信息，其存放的地址(称为散列地址)是由用户在原信息中选出的关键字(key)或关键字函数 f(key)的计算结果而决定的。如果不同关键字得到同一散列地址称为冲突，应尽量避免。图 5.7 所示为哈希表(即散列表)示意图。

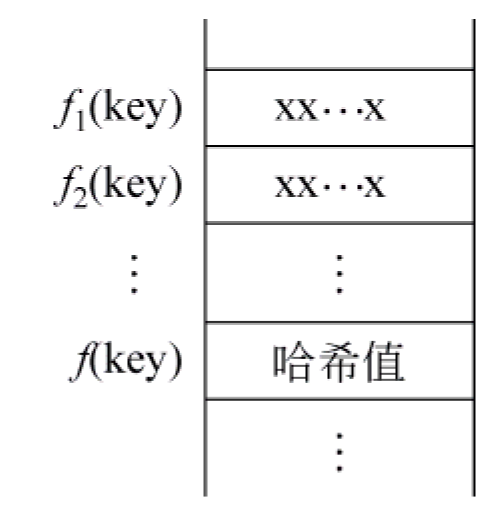


图 5.7 哈希表示意图

2. 哈希值(即摘要信息)的生成

目前从原信息生成摘要信息一般采用 MD5 算法(Message Digest Algorithm 5，信息摘要算法第 5 版)或 SHA-1 算法(Secure Hash Algorithm-1，安全散列算法-1)，其实现步骤可参阅相关的工业标准。SHA-1 算法能将 2^{64} 位(最大值)信息生成固定为 160 位的摘

要信息。MD5 的摘要信息长度为 128 位(32 个十六进制数)。

如果两个不相等的原信息生成相同的摘要信息,也称为冲突,应尽量避免,或者改进算法。对算法的基本要求之一是:原信息与其摘要信息的表示形式是混杂的,即不容易分析出两者的关系,即使原信息中数据仅修改了一位,其摘要信息变化很大,让人感到篡改信息不容易。

3. 哈希表的处理与查找

将上述的哈希值存放在存储器的散列地址中。在存放时,如果发现该散列地址已被占用,则将其存放在下一个散列地址中。

查找:如果要得到某一原信息的哈希值,首先根据原信息的关键字函数计算得到散列地址,到散列地址中取出哈希值,或者到下一个散列地址中取得。

由于 Hash 算法属于单向密码体制,因此当接收方接收到原信息和哈希值时,按同样方法根据原信息计算出哈希值,并与发送来的哈希值进行比较,如果相等,说明传送的原信息无差错或未被干扰;否则说明有错。

5.3.4 数据的安全保证

为保护数据的安全,采取防窃密、防篡改、防攻击、防瘫痪和防病毒措施。例如,在军事上防止情报泄密和被篡改,在民用上防止盗窃和经济上的损失。计算机病毒有以下特点:寄生性(寄生在某程序中,当执行该程序时起破坏作用)、传染性、潜伏性、隐蔽性、破坏性和触发性(当遇到特定条件时,触发病毒发作)。

1. 数字证书和电子签证机关

数字证书用来证实一个单位的身份和对网络资源的访问权限。由一个有信誉的公正权威机构——认证机构(Certificate Authority,CA)——向申请单位发放证书,证书是一个数字文件,除包括单位负责人的姓名、地址、证书序号和有效期、单位持有的公钥及发证单位(CA)的数字签名(将上述信息绑在一起经过 CA 的私钥加密后的信息称为 CA 签名)外,还向单位发放一对密钥(公钥和私钥)。

如果传送报文时发生纠纷,CA 利用单向函数(哈希函数)对传送的报文进行处理,鉴别报文的真伪。

方法如下:将报文的摘要信息用发送者(甲方)的私钥加密,与原文一起传送给接收者,接收者(乙方)用哈希函数产生原文的摘要信息,并用发送者的公钥来解密已被加密的摘要信息,如果两者(摘要信息)相同,说明甲方发送的信息是完整的,没有被修改。

CA 的作用是签发证书和管理证书、密钥。

证书上的 CA 签名实际上是经过 CA 私钥加密的信息。一个单位想鉴别另一个单位证书的真伪可用 CA 的公钥对该单位证书上的 CA 签名解密,如果结果与证书上的内容(姓名、地址等)一致,则说明证书是真的,从而验证了被鉴别单位的身份。

传送报文时,报文中有了发送方的数字签名后,不能否认该报文是他发送的。

2. 公钥基础设施

公钥基础设施(Public Key Infrastructure, PKI)为网络应用提供加密和数字签名等密码服务,以及密钥和证书的签发和管理设施。

3. 网络信息安全

网络信息安全涉及网上信息的保密性、完整性、可用性、真实性和可控性的相关技术和理论。在网络运行方面要求对信息的读写和传输等操作受到保护和控制，防止非法窃取信息和篡改信息，防止病毒的侵犯和用户应用程序的瘫痪。

从网络安全服务角度出发，除了实现智能卡安全需要解决的问题外，还应该采用防火墙技术。

(1) 防火墙。防火墙是由软、硬件构成的设备，是一种特殊编程的路由器，用来在两个网络之间实施接入控制策略。互联网防火墙是增强机构内部网络安全的系统，该系统决定了哪些内部服务可以被外界访问，又有哪些外界对象可以访问内部的哪些服务，内部人员又能访问哪些外部服务。进出互联网的信息都必须经过防火墙进行检查，防火墙只允许授权的数据通过。

(2) 防病毒。计算机病毒是隐藏在存储器中蓄意破坏的程序，具有可运行、复制、传染、潜伏、欺骗和顽固等特点，其特点可分为以下类型。

① 操作系统型。病毒程序取代操作系统中的某些模块，在引入操作系统时就进入主存储器。

② 入侵与包围型。该类病毒程序包围着某些主体程序(称为宿主程序)，当宿主程序运行时，病毒程序就入侵到主程序内部进行扰乱。

③ 源码型。病毒程序在高级语言程序被编译前已入侵源程序。最初病毒程序寄生在某个程序中，处于静止状态，一旦被引导或调用，就被激活，传染给其他软件，干扰系统的正常运行。

病毒的入侵与反入侵的对抗，是一场长期的斗争，目前国内外已有不少抗病毒的软件，取得良好的检测和预防作用。

5.3.5 密钥管理

无论在智能卡中采用哪种密码体制，都要考虑一个重要的问题，就是密钥的管理。密钥是一个加密系统中的可变部分，在现代密码学公开加密算法的前提下，密钥成为加密系统的关键，如果攻击者获得密钥，那么很容易从截取到的密文得出明文。因此，密钥管理也就具有了极其重要的地位。

密钥管理是一门综合性的技术，它涉及密钥的产生、检验、分配、传递、保管、使用和销毁的全部过程，并且与密钥的行政管理制度及人员的素质密切相关。目前，国际标准化组织也已经开展密钥管理标准化的工作，并制定了密钥管理标准 DIS-8732。不过总的来说，对应于具体的系统往往会有具体的实际要求，因此标准化工作事实上很难统一。

现在的密钥管理系统一般采取层次结构，其基本思想是用密钥来保护密钥，即用第 i 层的密钥 K_i 来保护第 $i+1$ 层的密钥 K_{i+1}，同时 K_i 本身也受到第 $i-1$ 层的密钥 K_{i-1} 的保护。至于具体应该设计成几层，则由密钥管理系统的功能来确定。功能越简单，层次就可以越少；反之就可以适当增加层数。采用这种分层模式可以大大提高安全性。由于下层的密钥内容可以设计成按某种协议而不断变化，从而使整个密钥管理系统表现为一种动态的特征。

下面以三层次密钥管理系统为例予以说明。三层次结构如下。

主密钥——→子密钥——→会晤密钥
（1）　　　（2）　　　（3）

在智能卡和读写器中存放相同的主密钥（假设为对称密码体制），主密钥可以是一个也可以是多个。由主密钥对某些指定的数据（一般是可变的）进行加密后生成子密钥，然后用子密钥对另外一些指定数据（一般也是可变的）进行加密，加密的结果即为会晤密钥。假如智能卡与读写器之间传送的数据需要加密，就用会晤密钥进行加密，会晤密钥仅使用一次，这样即使一旦会晤密钥被破译，也仅对一次已传送的数据有效，同时，从会晤密钥要解出主密钥也是非常难的。如何保证会晤密钥被使用一次呢，这要从会晤密钥的生成方式讲起。一般在 IC 卡内设置有芯片制造商标识码、卡的序列号或应用序列号等，其中卡的序列号（或应用序列号）是各卡都不相同的。另外，在每次交易时，往往还记录下交易时间（时间的最小单元应该是“s”），某些卡内还可能设置计数器，当卡内执行某条命令或完成一次交易时将该计数器加 1，这就保证了每进行一次交易，交易时间或计数器都是各不相同的。于是可以这样设计，用主密钥对卡的制造商标识码、卡的序列号或应用序列号进行加密生成子密钥，这样虽然使用同一主密钥，但各卡生成的子密钥是不相同的。然后用子密钥对交易时间或计数器进行加密生成会晤密钥，这样即使对同一张卡，每次交易所用到的会晤密钥也是不同的。再加上不同的交易可能使用不同的主密钥，或者一次交易用到几个主密钥，这实际上使得破译工作的难度很大，破译的意义不大。

DES 算法在 IC 发展到今天的情况下，要破译出密钥的时间已大大缩短。但是当采用了 DES 算法，而且密钥（上述的会晤密钥）变更极快的情况下，其安全性还是有保证的。

上面介绍了三层次密钥生成的办法，需要指出的是，这种方法不是唯一的。下面要讨论一下主密钥是如何生成和下载到读写器和 IC 卡的。

主密钥可由几个可信任的人彼此独立提出的数据组合成一个密钥（单长度或双长度），然后对某个数据（如随机数）进行加密运算而获得，这样主密钥的生成与变化规律也就很难被其中某个人预估了。

主密钥的下载过程稍有不慎，就有可能被泄露，因此下载的环境应是安全的。

主密钥下载到 IC 卡一般在个人化时进行，个人化是在专门的设备上进行的，下载时的环境应是安全的，要保证 IC 卡触点上的信息不能被窃取，主密钥下载到卡内以后就不能再读到芯片以外，这一般由卡内芯片特有的硬件（熔丝）和软件（COS 卡内操作系统）来保证。上述个人化的专门设备应严格保管好，操作人员要验证身份后才能进行操作。

向读写器设备下载主密钥存在一些问题。若采取和 IC 卡同样的方法，则要将相对比较笨重的读写器带到指定处进行下载，而且很难保证密钥写入后不能再读出，因为它不具备 COS 功能。经常采取的有效办法是使用安全存取模块（Secure Access Module，SAM），在该模块内下载有密钥，并能实现相应的加密/解密算法。SAM 可安全生产，将 SAM 安装在读写器中，读写器要执行的一切加密/解密运算都在 SAM 中进行。SAM 中的密钥不会泄露，而且有特殊保护功能，当受到攻击时可自动擦除模块内的信息。

5.4　智能卡的安全使用

智能卡主要用于验证身份或作为支付工具(如银行发的电子钱包/电子存折或公交等系统发的预付费卡),在使用时读写器与 IC 卡要相互确认,以防止伪卡或插错卡。一般来说,使用一次卡要经历以下步骤(以接触式卡为例)。

(1) 插卡。读写器向卡加电源,并发一复位信号 RST,令卡进行初始化,做好交易的准备,然后由卡发出复位应答信号 ATR(见第 4 章)。

(2) 读写器鉴别卡的真伪。

(3) 卡鉴别读写器的真伪。

(4) 检查此卡是否列入黑名单,如已列入,将停止使用。

(5) 检查上次交易是否已正常完成。如果上次在完成前就拔卡或断电,卡应具有自动恢复数据的功能。

(6) 鉴别持卡人的身份。通常采用密码比较方法,即由持卡人输入只有他本人知道的密码 PIN,与预先存在卡内的密码进行比较,如比较相符,说明持卡人是卡的主人。但也有可能是伪持卡人窃得了卡与密码,所以更严格的要求可采用生物特征来验证,如照片、指纹等。

(7) 根据应用需求进行交易或验证通行。这时可能要对数据的可靠性和完整性进行检查(视需要而定),数据也可能需要加密传送。

(8) 拔卡。

以上各步骤的顺序可以有变动。随着命令系统的不同,执行步骤和内容也会随之而异。如果在交易未正常完成时,发生断电或拔卡情况,卡内的有用数据不应改变,卡的功能不会受损。

下面介绍读写器与 IC 卡相互鉴别的方法。

(1) IC 卡鉴别读写器的真伪。先由读写器向智能卡发一取口令(产生随机数)命令,卡产生一随机数 R,然后由读写器对随机数加密成密文 M,密钥是预先存放在读写器和 IC 卡中的,密钥的层次按需要而定。读写器将密文与外部鉴别命令送到 IC 卡,卡执行命令时将密文解密成明文 R',并将明文和原随机数比较,如果相同,卡承认读写器是真的,否则卡认为读写器是伪造的。其原因简述如下。

如果采用 DES 算法进行加密/解密运算,那么存放在智能卡和读写器中的密钥是相同的,而且是保密的,是不让第三方知道的。如果先进行加密、再进行解密后的结果与加密前的数据相同,说明读写器内的密钥是正确的,读写器也是真的(伪造的读写器无法取得正确的密钥),这再一次说明了密钥要严格保密。

下面来描述智能卡鉴别读写器的过程。

如图 5.8 所示,左半部表示读写器进行的操作,右半部表示智能卡进行的操作。智能卡的操作是完全按读写器发出的命令进行的。采用随机数的原因也是为了安全。

(2) 读写器鉴别 IC 卡的真伪(图 5.9)。其原理与卡鉴别读写器真伪相似,但使用内部鉴别命令,解密后的结果与随机数进行比较的操作应在读写器中进行,显然不能由 IC

卡来判断自身的真伪。

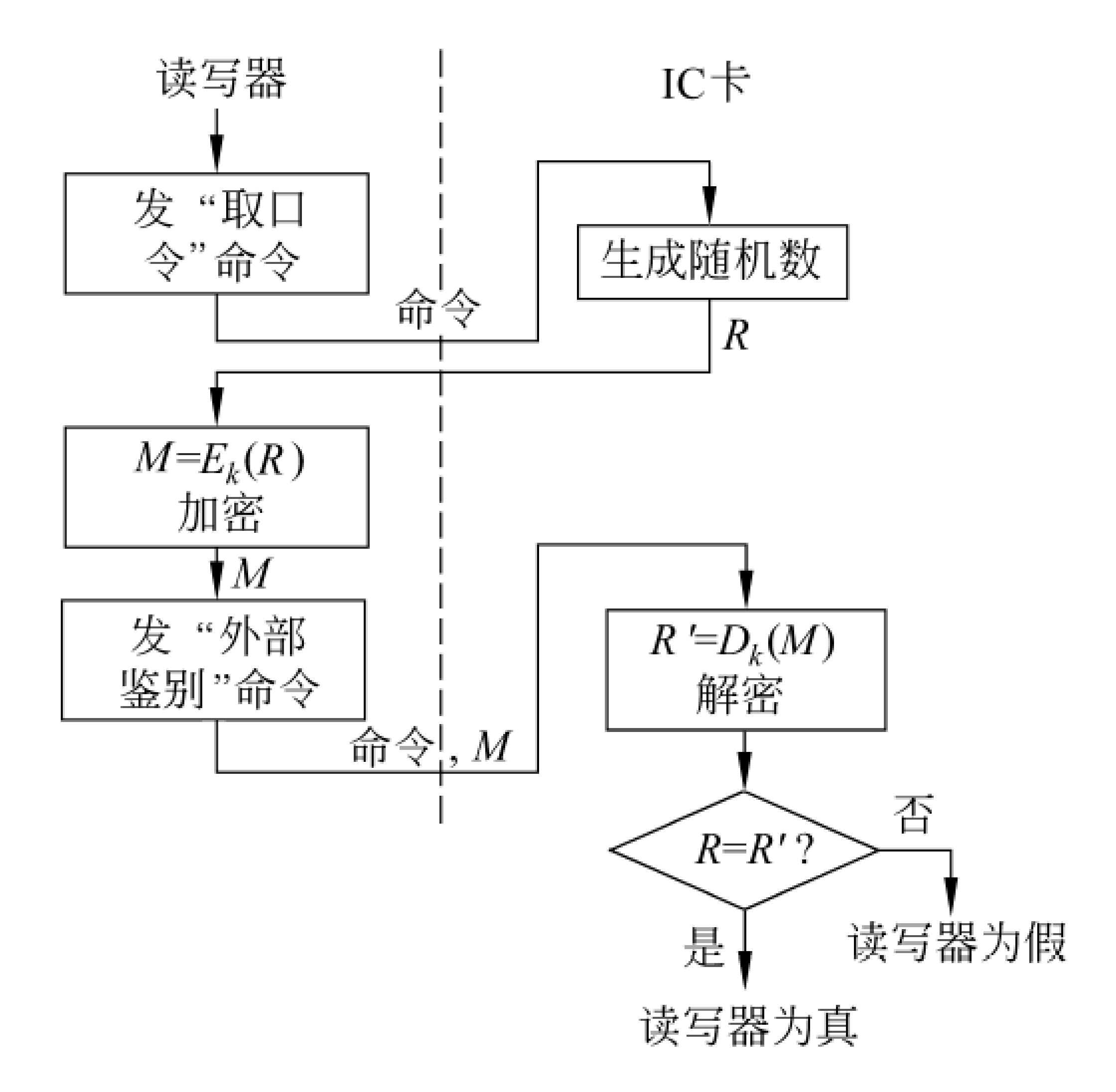



图 5.8　IC 卡鉴别读写器的真伪

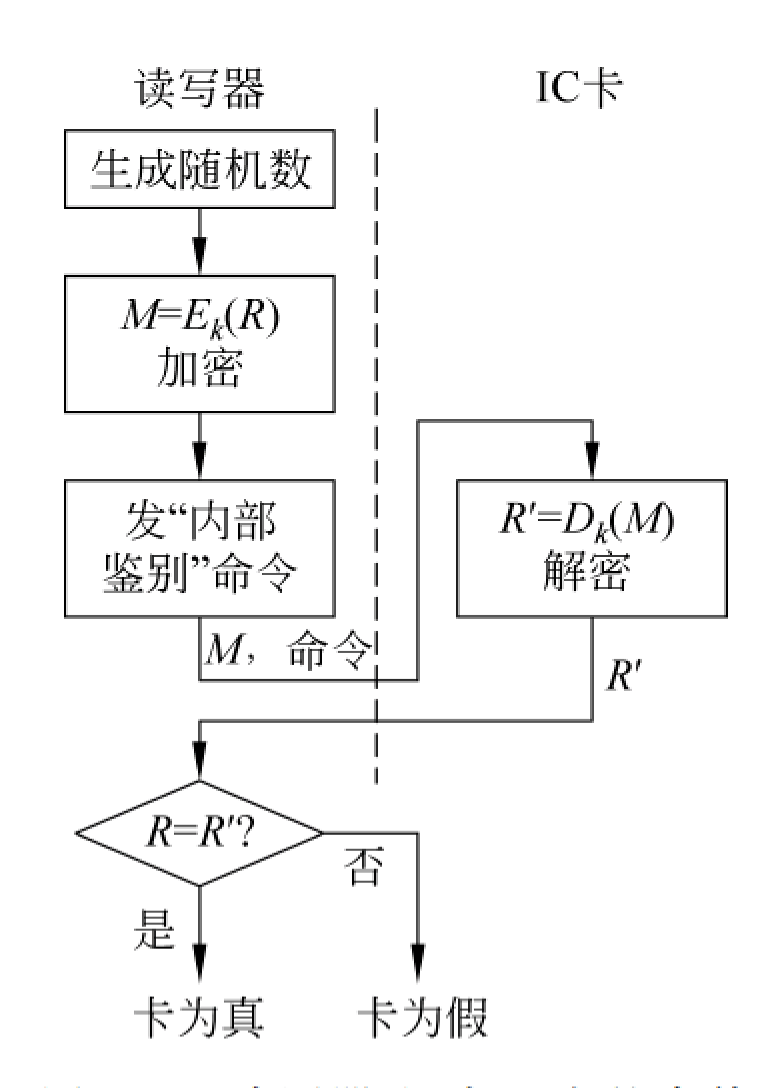


图 5.9　读写器鉴别 IC 卡的真伪

取口令命令、外部鉴别命令和内部鉴别命令的功能见第 6 章。

通过 IC 卡触点的信息是容易被窃取的，非接触式 IC 卡与读写器之间传送的信息更容易被窃取。

习题

1. 对智能卡的安全造成威胁的行为有哪些？
2. 说出为验证持卡人是否是假冒的而经常采取的验证方法。
3. 如果持卡人多次输入 PIN，但都不正确，将发生什么情况？
4. 说明智能卡和读写设备之间相互认证的方法，即如何确定对方是真实的而不是伪造的。
5. 为了保证在系统中交换的信息报文不被篡改而在报尾增加鉴别码的作用及产生方法是什么？
6. DES 加密算法属于何种密码体制？它的主要特点是什么？加密与解密过程怎样？
7. 说明多重 DES 算法的意义及其实现方法。
8. RSA 加密算法属于哪种密码体制？它的主要特点是什么？加密与解密过程怎样？
9. 在智能卡和读写设备之间相互认证时，通常采用发送随机数而不是固定数的方法，这是为什么？
10. 什么是数字签名？
11. 认证机构 CA 的作用是什么？
12. 根据 DES 算法和 RSA 算法的具体实现，对卡内 CPU 硬件有什么不同的要求？
13. 密钥管理的作用是什么？

第 6 章　智能卡的命令系统

当卡和读写器成功地建立起联系以后，就需要通过可靠、安全的数据交换，以实现具体的应用目标。

本章综合了 ISO/IEC 7816 下属的多个标准的内容，其重点是安全体系和命令-响应对。上述各标准不是同时发表的，并有多次改动。在实际的应用领域中，采用标准的命令和自己新设计的命令都是存在的。

6.1　智能卡和读写器之间的命令-响应对

命令和响应必成对出现，即从读写器向卡发送的一个命令 APDU（Application Protocol Data Unit，应用协议数据单元）跟随着从卡向读写器发回的一个响应 APDU。

命令-响应对的格式如下。

命令 APDU

类别 CLA	命令码 INS	参数 P1-P2	Lc	数据	Le	
1	1	2	0，1，3	$0\sim N$	0，1，2，3	字节

响应 APDU

数据	SW1-SW2	
$0\sim N$	2	字节

在命令 APDU 中，CLA、INS 和 P1-P2 指出卡要完成的操作及其参数，Lc 指出读写器发往卡的数据长度，Le 是期望卡发回的响应数据长度。在响应 APDU 中，SW1-SW2 是由卡返回的状态，表示命令已完成或出现差错的情况。

Lc 字段的长度有两种：短长度（0 或 1 个字节）和扩展长度（3 个字节）。Le 字段的长度也有两种：短长度（0 或 1 个字节）和扩展长度（2 或 3 个字节）。如果在命令 APDU 中 Le 字段的编码为 N_e，而在响应 APDU 中返回的数据为 N_r 个字节，且 $N_r<N_e$，这说明还有（N_e-N_r）个字节需要返回，其差值将在响应 APDU 的状态字节（SW1-SW2）中反映出来。读写器接收此信息后，将进一步发送相关命令（GET RESPONSE 命令）要求继续返回余下的数据，从而完成数据传送的链接功能。

在所有的命令-响应对中，如果 Le 字段不存在，表示没有响应数据字段。

如果命令处理失败，响应 APDU 中的响应数据字段应不存在，并且 SW1-SW2 应指出一个差错。

参数字节 P1-P2 指出处理命令的控制和选项。参数字节的编码和含义在每条命令中

介绍。

类别字节 CLA、指令字节 INS 和状态字节 SW1-SW2 在下面说明。

1. 类别字节 CLA

CLA 指示命令的类别。

CLA＝000××××× 和 01×××××× 是在本标准中定义的类别。其他值保留供将来使用。

1）表 6.1 规定了 CLA＝000××××× 时各位的定义

- b_8、b_7、b_6 置为 000。
- b_5 控制命令链。
- b_4 和 b_3 指明安全报文传输。
- b_2 和 b_1 是编码为 0～3 的逻辑通道号。逻辑通道的意义已在 2.1.4 节说明，其使用和卡内操作系统 COS 有关。

表 6.1　CLA＝000×××××

b_8	b_7	b_6	b_5	b_4	b_3	b_2	b_1	含　义
0	0	0	×	—	—	—	—	命令链控制
0	0	0	0	—	—	—	—	• 本命令是命令链的最后一条或命令链仅此一条命令
0	0	0	1	—	—	—	—	• 本命令不是命令链的最后一条
0	0	0	—	×	×	—	—	安全报文传输 SM 指示
0	0	0	—	0	0	—	—	• 无 SM 或无指示
0	0	0	—	0	1	—	—	• 专用 SM 格式
0	0	0	—	1	0	—	—	• 命令头不参与鉴别
0	0	0	—	1	1	—	—	• 命令头参与鉴别
0	0	0	—	—	—	×	×	0～3 的逻辑通道号

注：×表示本位有 0 和 1 两种情况；—表示本位不起作用(下同，不再说明)。

2）表 6.2 规定了 CLA＝01×××××× 时各位的定义

- b_8 和 b_7 置为 01。
- b_6 指明安全报文传输。
- b_5 控制命令链。
- b_4～b_1 编码为 0～15，该值加上 4 即为 4～19 的逻辑通道号。

表 6.2　CLA＝01××××××

b_8	b_7	b_6	b_5	b_4	b_3	b_2	b_1	含　义
0	1	×	—	—	—	—	—	安全报文传输 SM 指示
0	1	0	—	—	—	—	—	• 无 SM 或无指示
0	1	1	—	—	—	—	—	• 命令头不参与鉴别
0	1	—	×	—	—	—	—	命令链控制
0	1	—	0	—	—	—	—	• 本命令是命令链的最后一条或命令链仅此一条命令
0	1	—	1	—	—	—	—	• 本命令不是命令链的最后一条
0	1	—	—	×	×	×	×	4～19 的逻辑通道号

3）说明(对表 6.1 和表 6.2 的解释)

(1) 安全报文传输指的是利用加密和认证码来保护命令-响应对，否则是用明文来表示命令-响应对。

(2) 命令链。命令链规定了多条相邻的命令-响应对可以被链接在一起的机制，该机制可以在执行多步处理时使用。例如，当单一命令传输的数据串过长时(即前面提到的 $N_r < N_e$ 的情况)可采用命令链，即连续用多条命令实现数据的传送。

如果 CLA 的 b_5 为 1，表示该命令不是命令链的最后一条命令。

(3) 逻辑通道。

- CLA 指出：读写器和 IC 卡在执行本条命令时命令-响应对的通道号。
- 基本通道始终可用，即它不能被关闭。它的通道号为 0。其他通道可由命令打开或关闭。
- 不支持多个逻辑通道的卡仅使用基本通道。
- 在同一时刻，仅有一个通道可用，该通道称为当前通道。
- 如果命令中 CLA 指出的通道尚未开放，则该命令无效。

2. 指令字节 INS

INS 指明要操作的命令，根据 ISO/IEC 7816-3 的规定，值'6X'和'9X'是无效的。

表 6.3 列出了 ISO/IEC 7816 中规定的大部分命令。每条命令的格式、功能等在 6.3 节中描述。

表 6.3 ISO/IEC 7816 中规定的命令

序号	命令名称	INS	定义于
1	CREATE FILE 创建文件	'E0'	7816-9
2	SELECT(FILE)选择文件	'A4'	7816-4
3	MANAGE CHANNEL 管理通道	'70'	7816-4
4	DELETE FILE 删除文件	'E4'	7816-9
5	DEACTIVATE FILE 暂停文件	'04'	7816-9
6	ACTIVATE FILE 激活文件	'44'	7816-9
7	TERMINATE DF 终止 DF	'E6'	7816-9
8	TERMINATE EF 终止 EF	'E8'	7816-9
9	TERMINATE CARD USAGE 终止卡使用	'FE'	7816-9
10	READ BINARY 读二进制	'B0', 'B1'	7816-4
11	WRITE BINARY 写二进制	'D0', 'D1'	7816-4
12	UPDATE BINARY 更新二进制	'D6', 'D7'	7816-4
13	SEARCH BINARY 搜索二进制	'A0', 'A1'	7816-4
14	ERASE BINARY 擦除二进制	'0E', '0F'	7816-4
15	READ RECORDS 读记录	'B2', 'B3'	7816-4

续表

序号	命 令 名 称	INS	定义于
16	WRITE RECORD 写记录	'D2'	7816-4
17	UPDATE RECORD 更新记录	'DC', 'DD'	7816-4
18	APPEND RECORD 增加记录	'E2'	7816-4
19	SEARCH RECORD 搜索记录	'A2'	7816-4
20	ERASE RECORDS 擦除记录	'0C'	7816-4
21	INTERNAL AUTHENTICATE 内部鉴别	'88'	7816-4
22	GET CHALLENGE 取口令	'84'	7816-4
23	EXTERNAL AUTHENTICATE 外部鉴别	'82'	7816-4
24	GENERAL AUTHENTICATE 综合鉴别	'86', '87'	7816-4
25	VERIFY 验证	'20', '21'	7816-4
26	CHANGE REFERENCE DATA 替换引用数据	'24'	7816-4
27	ENABLE VERIFICATION REQUIREMENT 允许验证要求	'28'	7816-4
28	DISABLE VERIFICATION REQUIREMENT 禁止验证要求	'26'	7816-4
29	RESET RETRY COUNTER 复位重试计数器	'2C'	7816-4
30	PERFORM SECURITY OPERATION 完成安全操作	'2A'	7816-8
31	GENERATE PUBLIC KEY PAIR 生成公开密钥对	'46'	7816-8
32	GET RESPONSE 获取响应	'C0'	7816-4
33	PERFORM TRANSACTION OPERATION 事务管理操作	'12'	7816-7
34	PERFORM USER OPERATION 用户管理操作	'14'	7816-7
35	APPLICATION MANAGMENT REQUEST 应用管理请求	'40','41'	7816-13
36	LOAD APPLICATION 加载应用	'EA','EB'	7816-13
37	REMOVE APPLICATION 删除应用	'EC','ED'	7816-13

INS 的 b_1 指明数据字段格式，具体如下。

- 如果 b_1 置为 1(奇数 INS 代码)，则数据字段按 BER-TLV 编码。
- 如果 b_1 置为 0(偶数 INS 代码)，则不提供数据字段格式的指示。

3. 状态字节 SW1-SW2

SW1-SW2 指示了处理状态。所有不同于'6XXX'和'9000'的值都是无效的。此外，值'60XX'也是无效的。

图 6.1 所示为用于 SW1-SW2 的值'9000'和'61XX'到'6FXX'的结构化图解。

表 6.4 列出了 SW1-SW2 的值及其通常的含义。

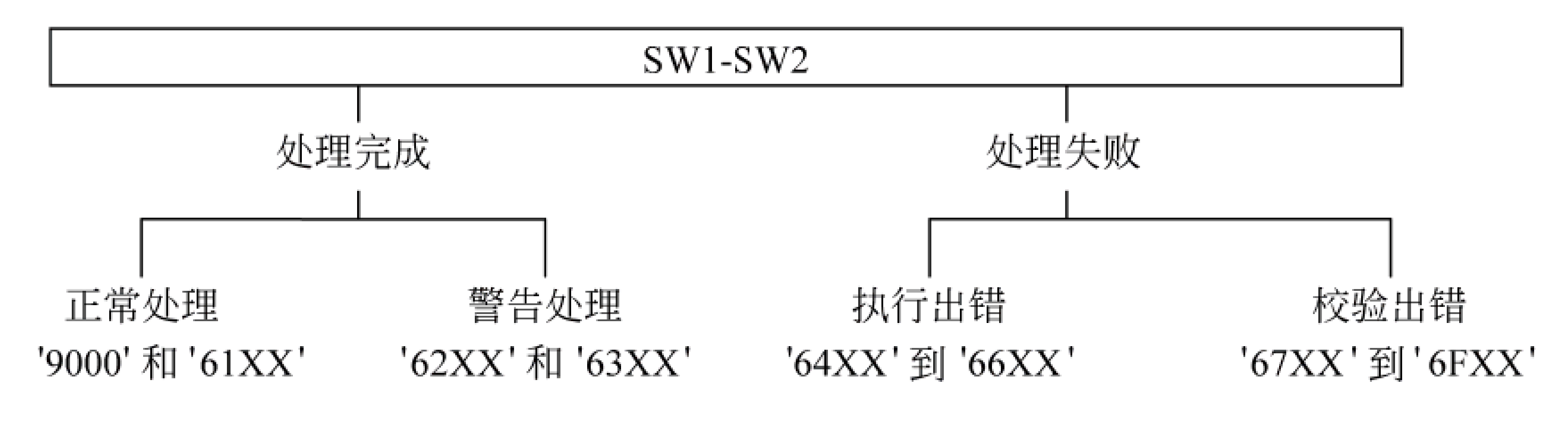


图 6.1　SW1-SW2 值的结构化图解

表 6.4　SW1-SW2 的值及通常含义

操　作	SW1-SW2	含　　义
正常处理	'9000'	
	'61XX'	SW2 编码表示仍然可以获取的数据字节数(见下面文本)
警告处理	'62XX'	非易失存储器状态无变化(在 SW2 中进一步说明情况)
	'63XX'	非易失存储器状态变化(在 SW2 中进一步说明情况)
执行出错	'64XX'	非易失存储器状态无变化(在 SW2 中进一步说明情况)
	'65XX'	非易失存储器状态变化(在 SW2 中进一步说明情况)
	'66XX'	安全相关的发布
校验出错	'6700'	错误的长度
	'68XX'	CLA 中的功能不被支持(在 SW2 中进一步说明情况)
	'69XX'	不允许的命令(在 SW2 中进一步说明情况)
	'6AXX'	错误的参数 P1-P2(在 SW2 中进一步说明情况)
	'6B00'	错误的参数 P1-P2
	'6CXX'	错误的 Le 字段。SW2 编码准确的有效数据字节数(见下面的文本)
	'6D00'	指令代码不被支持或无效
	'6E00'	类别不被支持
	'6F00'	没有精确的诊断

如果处理失败,返回 SW1 为'64'～'6F',则没有响应数据字段。

(1) 如果 SW1 置为'61',则处理完成,在发送其他命令之前,可以先发送与之有相同 CLA 且 SW2(仍然有效的数据字节数)作为短 Le 字段的 GET RESPONSE 命令。

(2) 如果 SW1 置为'6C',则处理失败,在发送其他命令之前,可以重新发送原有命令,SW2(确切的有效字节数)为短 Le 字段。

表 6.5 列出了 ISO/IEC 7816 中使用的所有警告和错误情形。

表 6.5　警告和错误情形

SW1	SW2	含　　义
'62'(警告)	'00'	没有信息被给出
	'02'～'08'	由卡发起的查询
	'81'	返回数据的一部分,数据可能被损坏
	'82'	读出 N_e 字节之前文件或记录已结束
	'83'	选择的文件无效
	'84'	FCI 未按照 3.3.2 节格式化
	'85'	选择的文件为终止状态
	'86'	没有来自卡传感器的有效数据

续表

SW1	SW2	含　　义
'63'(警告)	'00'	没有信息给出
	'81'	文件被上一次写入填满
	'CX'	通过'X'(值为0～15)提供的计数器(正确的含义依赖于命令)
'64'(错误)	'00'	运行出错
	'01'	卡需要返回数据
	'02'～'80'	由卡发起的查询
'65'(错误)	'00'	没有信息给出
	'81'	存储器故障
'68'(错误)	'00'	没有信息给出
	'81'	逻辑通道不被支持
	'82'	安全报文不被支持
	'83'	期望是命令链的最后一条命令
	'84'	命令链接不被支持
'69'(错误)	'00'	没有信息给出
	'81'	命令与文件结构不兼容
	'82'	安全状态不满足
	'83'	鉴别方法被阻塞
	'84'	引用的数据无效
	'85'	使用的条件不满足
	'86'	命令不被允许(无当前 EF)
	'87'	期望的 SM 数据对象失踪
	'88'	SM 数据对象不正确
'6A'(错误)	'00'	没有信息给出
	'80'	在数据字段中的不正确参数
	'81'	功能不被支持
	'82'	文件或应用未找到
	'83'	记录未找到
	'84'	无足够的文件存储空间
	'85'	N_c 与 TLV 结构不一致
'6A'(错误)	'86'	不正确的参数 P1-P2
	'87'	N_c 与 P1-P2 不一致
	'88'	引用的数据未找到(正确的含义依赖于命令)
	'89'	文件已存在
	'8A'	DF 名已存在
其他所有 SW2 的值均被 ISO/IEC JTC1/SC17 定义为 RFU		

6.2 智能卡的安全体系结构

6.2.1 安全状态、安全属性和安全机制

1. 安全状态

安全状态表示 IC 卡与安全有关的当前状态，如持卡人是否合法、读写器与卡是否已相互鉴别，卡的某些操作在满足一定的安全条件时才能进行。

考虑了下列 4 种安全状态的设置。

(1) 全局安全状态。可以通过完成与 MF 相关的鉴别规程进行修改(如附属于 MF 的 password 或密钥的实体鉴别)。

(2) 应用安全状态。可以通过完成与应用相关的鉴别规程进行修改(如附属于指定应用的 password 或密钥的实体鉴别)、维护、恢复或被丢弃。这种修改只与鉴别规程所属的应用相关。如果使用了逻辑通道，则应用安全状态依赖于逻辑通道。

(3) 文件安全状态。可以通过完成与指定 DF 相关的鉴别规程进行修改(如附属于指定 DF 的 password 或密钥的实体鉴别)、维护、恢复或被丢弃，这种修改只与鉴别规程所属的文件相关。如果使用了逻辑通道，则文件安全状态依赖于逻辑通道。

(4) 命令安全状态。仅在执行使用安全报文传输和涉及鉴别的命令期间它才存在。

2. 安全属性

当卡执行命令或访问文件时必须满足的安全条件，称为安全属性。

3. 安全机制

为满足安全属性的需求而采取的措施(建立或增强 IC 卡的安全状态)。例如，第 5 章中的持卡人身份识别和读写器、IC 卡之间的真伪识别而采取的措施。数据的保密性可通过加密和解密来实现。处理的结果可以按照应用的要求记录到文件或指定的存储单元中。

6.2.2 安全报文(SM)

安全报文(Secure Messaging，SM)通过确保数据秘密性和数据鉴别这两个基本安全功能，来保护全部或部分命令-响应对的数据字段。每种安全机制包括密码算法、操作模式、密钥和参数(输入数据)，还经常包含初始数据。

数据明文与安全报文的关系可简单表示为：

数据	明文	
安全报文	密文	密码校验和

在 SM 字段中，每个 SM 数据对象(上下相关文类)的标记字段(标记奇偶)的最后一位(b_1)用于指示该 SM 数据对象是否包括在用于鉴别(密码校验和，或者数字签名)的数据元的计算中(b_1 为 1，奇标记数，表示包括；b_1 为 0，偶标记数，表示不包括)。

1. SM 数据对象

SM 数据对象如表 6.6 所示，标记 T 属于上下文相关类。

表 6.6　SM 数据对象(模板标记'7D')

标记 T	值　V
'80','81'	明文
'82','83'	密文
'89'	命令头(CLA INS P1 P2)
'8E'	密码校验和
'90','91'	哈希编码
'92','93'	证书
'99'	处理状态(SW1-SW2)
'9A','9B'	输入的用于数字签名计算的数据元
'9C','9D'	公钥
'9E'	数字签名
'A0','A1'	用于计算哈希编码的输入模板
'A2'	用于验证密码校验和的输入模板
'A4','A5'	用于鉴别的控制引用模板
'A6','A7'	用于密钥协商的控制引用模板
'A8'	用于验证数字签名的输入模板
'AA','AB'	用于哈希编码的控制引用模板
'AC','AD'	用于数字签名计算的输入模板
'AE','AF'	用于验证证书的输入模板(连接的值字段被签名)
'B4','B5'	用于密码校验和的控制引用模板
'B6','B7'	用于数字签名的控制引用模板
'B8','B9'	用于保证秘密性的控制引用模板

2. 密码校验和

计算密码校验和涉及一个初始值、密钥和分组加密算法或哈希函数。

假设数据字长 256 位(32B),分成 4 组(D_1、D_2、D_3、D_4),每组长度为 8B。密码校验和的生成如图 6.2 所示,初始值可选择'00'、随机数或其他值。

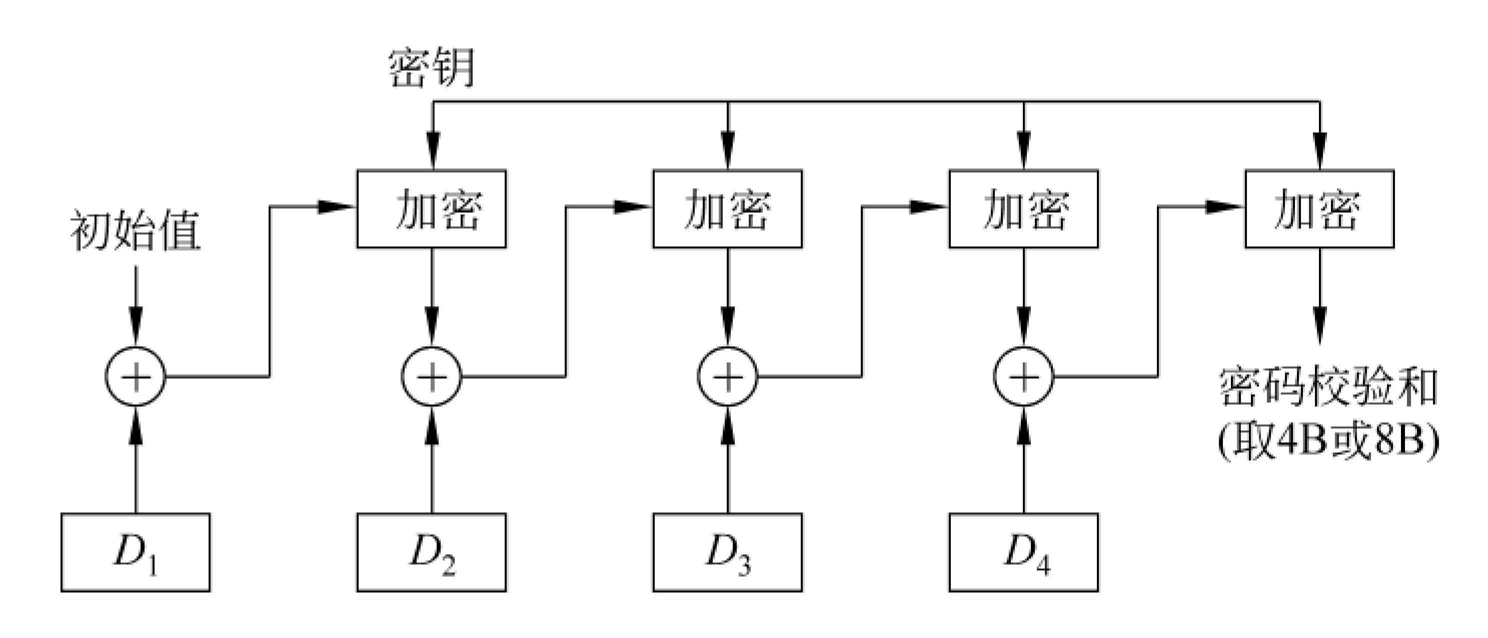


图 6.2　密码校验和的生成(举例)

6.3 智能卡的命令系统

本节规定的命令分为以下 6 组。主要参考 ISO/IEC 7816。

(1) 管理卡和文件的命令。

(2) 数据单元处理命令。

(3) 记录处理命令。

(4) 安全处理命令。

(5) 传输处理命令。

(6) 在多应用环境中的应用管理命令。

并不强制所有的卡都支持上述命令,而且上述命令一般还不能满足应用的全部需求。在执行命令和处理文件时必须考虑当前的安全状态是否满足安全属性的要求,在所有场合都应考虑,一般不再重复提醒。

6.3.1 管理卡和文件的命令

1. 文件的生命周期状态

无论是卡、文件还是其他对象,都可以有生命周期,ISO/IEC 7816 定义了 4 种基本生命周期状态,即创建状态、初始状态、操作状态(激活和暂停)和终止状态。表 6.7 所示为定义的生命周期状态(Life Cycle Status,LCS)字节。

表 6.7 生命周期状态字节

b_8	b_7	b_6	b_5	b_4	b_3	b_2	b_1	含义
0	0	0	0	0	0	0	0	没有信息给出
0	0	0	0	0	0	0	1	创建状态(01)
0	0	0	0	0	0	1	1	初始状态(03)
0	0	0	0	0	1	—	1	操作状态(激活)(05)
0	0	0	0	0	1	—	0	操作状态(暂停)(04)
0	0	0	0	0	1	1	0	终止状态(06)
不全为 0				×	×	×	×	专有的

文件 LCS 字节可以出现在文件的控制参数中,以标记'8A'引用(表 3.5)。

卡 LCS 字节可以出现在历史字符中,以标记'48'引用。

基本生命周期状态之间的转变(除了操作状态激活和暂停之间)是不可逆的,并且只能是从创建到终止。生命周期状态的变化可以用下列命令实现。

- CREATE FILE(创建文件)。
- ACTIVATE FILE(激活文件)。
- TERMINATE EF(终止 EF)。
- DELETE FILE(删除文件)。
- DEACTIVATE FILE(暂停文件)。

• TERMINATE DF(终止 DF)。
• TERMINATE CARD USAGE(终止卡使用)。

可以通过执行命令来设置生命周期状态的值。

图 6.3 所示为文件生命周期的状态转换图,但没有示出这些命令执行的条件。

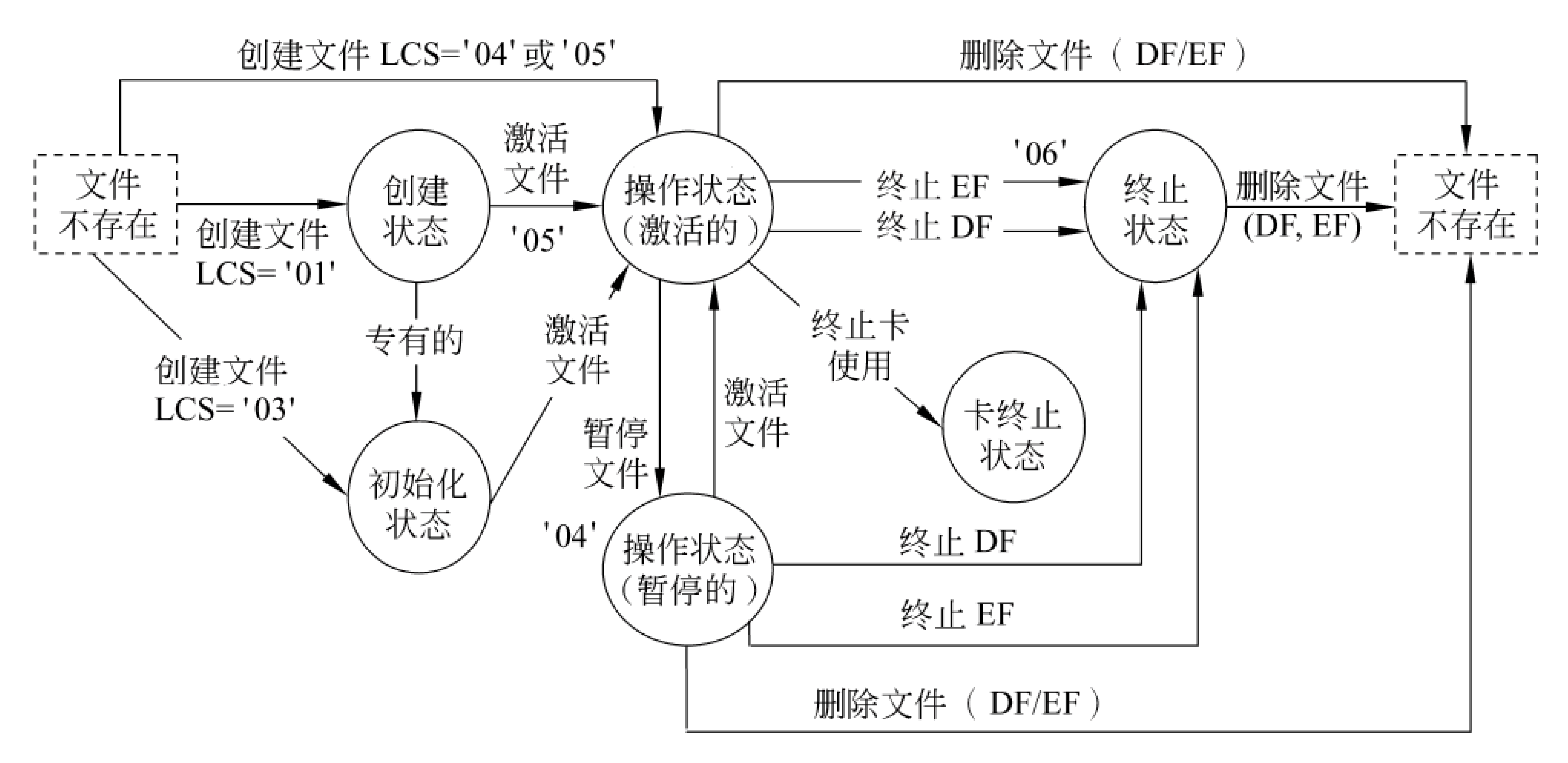


图 6.3 文件生命周期状态示意图

2. 用于卡管理的命令

1) CREATE FILE(创建文件)命令

CREATE FILE 命令创建一个文件(DF 或 EF),该文件直接处于当前 DF 下。在命令的数据字段给出被创建文件的文件名与 LCS 状态。该命令成功完成后,创建的文件将被置成当前文件,除非另有规定。当前文件是指处于操作状态(激活)的文件。

在同一个 DF 下不允许存在多个具有相同短文件标识符的 EF。

文件描述符字节是必备的,它指示创建了一个 DF 还是创建了一个 EF。

• 如果一个 DF 被创建,则应规定一个文件名和(或)一个文件标识符。
• 如果一个 EF 被创建,则应规定一个文件标识符和(或)一个短 EF 标识符。

CREATE FILE 命令的命令-响应对如下。

命令 APDU

CLA	'E0'	P1-P2	Lc	数据	
1	1	2	0,1,3	0～N	字节

P1-P2: 可以是文件标识符和文件描述字节或指出在数据字段的 FCP 模板中编码

Lc 字段: 其长度为 0B、1B 或 3B,与是否发送数据或发送的数据量有关

数据字段: FCP 模板(标记'62',表 3.5)或不存在(有默认文件控制参数)

响应 APDU

SW1-SW2	
2	字节

2) SELECT(选择)命令

在复位应答之后,通过基本逻辑通道选择 MF 或默认的应用 DF 作为当前文件。

SELECT 命令完成时，将打开由 CLA 所指定的逻辑通道，并在该逻辑通道中选择一个文件作为当前文件，后续命令可以通过该逻辑通道隐式地引用该当前文件。

选择的 DF(MF 或应用 DF)将成为该逻辑通道中的当前 DF。可以通过该逻辑通道来引用一个隐含的当前 EF。以前选择的 DF 将变成前一个当前 DF，并不再通过该逻辑通道引用。

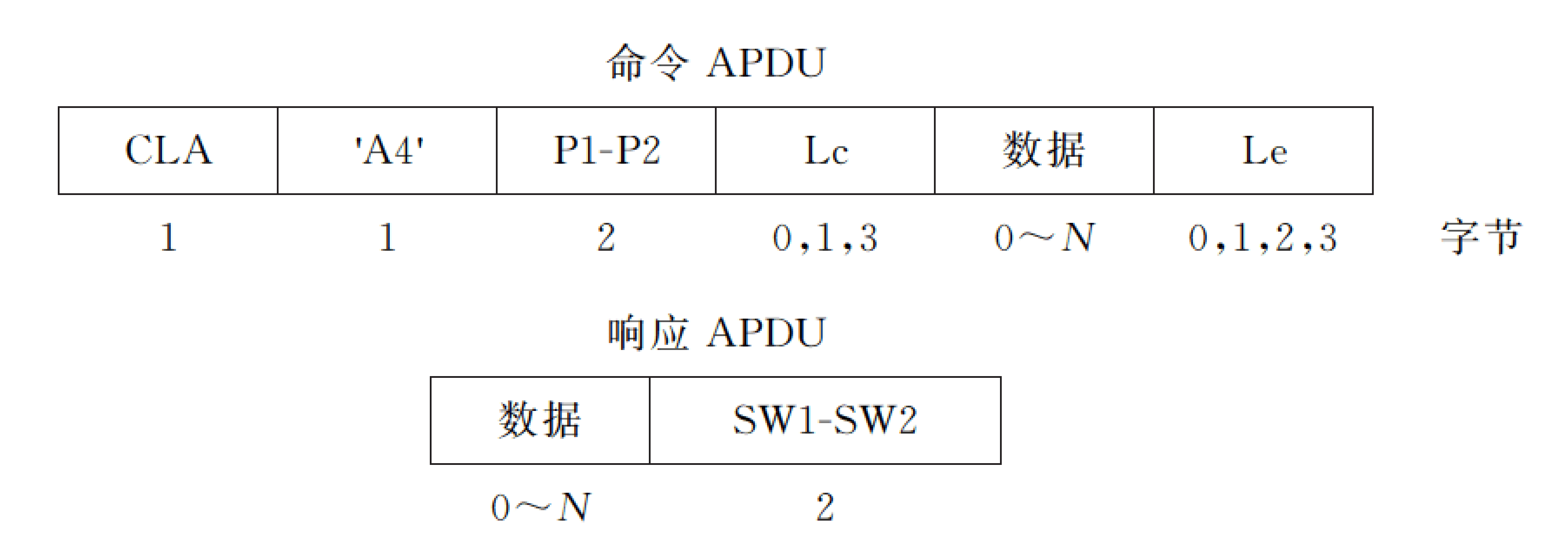
选择 EF 时设置了一对当前文件：EF 及其父 DF 文件。

除非另有规定，否则下面的规则将适用于一个 DF 层次结构中每个打开的逻辑通道。

(1) 如果当前 EF 被改变，或者在没有当前 EF 时，将失去针对前一个当前 EF 的安全状态。

(2) 如果当前 DF 是前一个当前 DF 的后代，或者与前一个当前 DF 是同一个 DF，则针对前一个当前 DF 的安全状态将保持不变；否则，针对前一个当前 DF 的安全状态将丢失。先前的和新的当前 DF 的所有共同祖先，所共用的安全状态将维持不变。

SELECT(FILE)命令参数 P1 和 P2 指出具体选择哪一种文件(MF、DF 或 EF)为当前文件(文件名由数据字段给出)，并指出响应数据字段是否返回或返回哪一种文件控制信息(FCP、FMD 或 FCI)。



命令 APDU

CLA	'A4'	P1-P2	Lc	数据	Le	
1	1	2	0,1,3	0～N	0,1,2,3	字节

响应 APDU

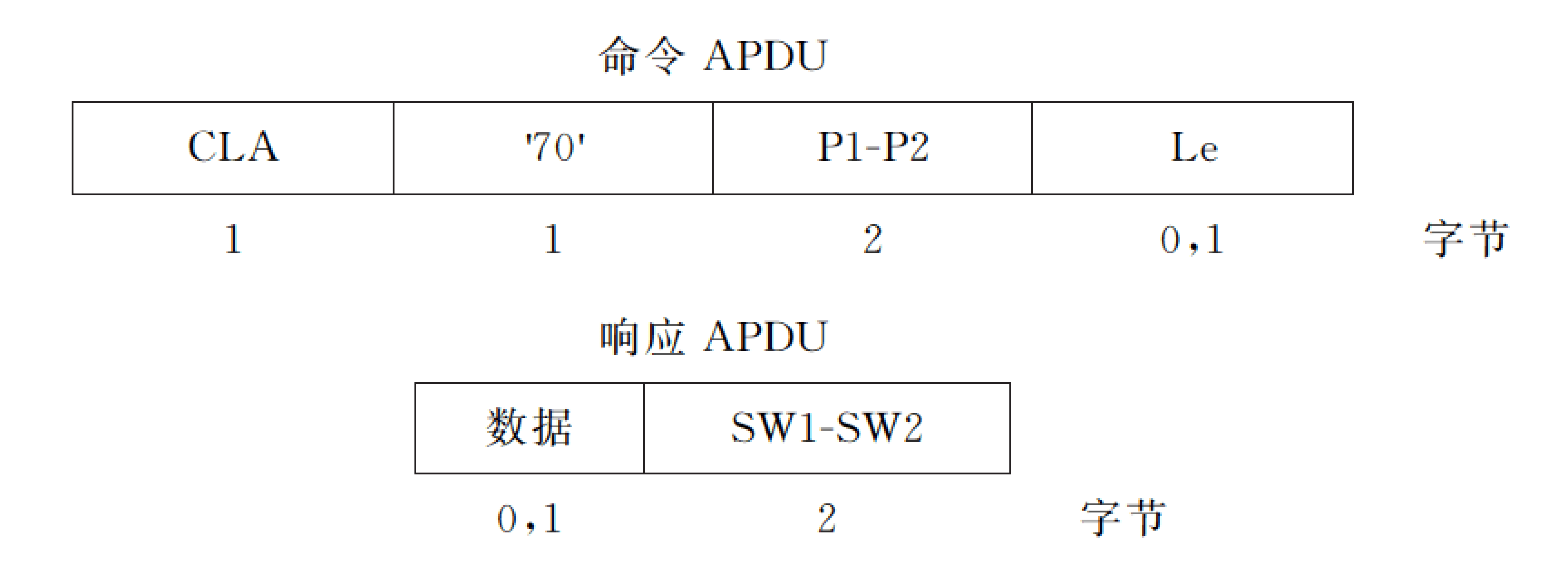
数据	SW1-SW2
0～N	2

3) MANAGE CHANNEL(管理通道)命令

MANAGE CHANNEL 命令打开或关闭除基本通道外的逻辑通道，即从 1～3 或 4～19 的通道号。

关闭后，该逻辑通道能够重新打开使用。

MANAGE CHANNEL 命令的命令-响应对如下。



命令 APDU

CLA	'70'	P1-P2	Le	
1	1	2	0,1	字节

响应 APDU

数据	SW1-SW2	
0,1	2	字节

由 P1-P2 指出打开或关闭的逻辑通道号，或者由响应的数据指出逻辑通道号。

4) DELETE FILE(删除文件)命令

DELETE FILE 命令删除直接处于当前 DF 之下指定的 EF，或者删除 DF 及其所有

的子文件。该命令成功完成后，删除的文件不能再被选择。在 EF 删除后，当前文件是当前 DF；在 DF 删除后，如果没有另外规定，当前 DF 是父辈 DF。文件所拥有的资源将被释放，并且该文件使用的存储空间将被置为逻辑擦除状态。

文件的删除还可能依赖于文件生命状态。MF 不允许被删除。

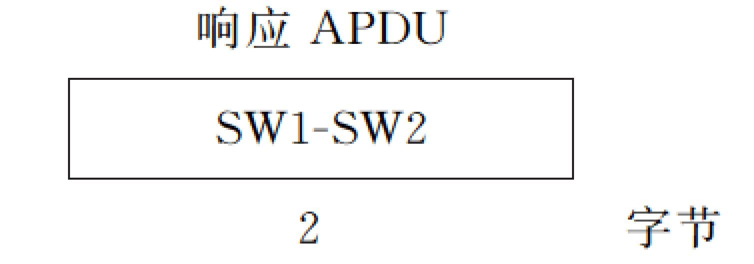
DELETE FILE 命令的命令-响应对如下。

命令 APDU

CLA	'E4'	P1-P2	Lc	数据	
1	1	2	0，1，3	N_c	字节

由 P1-P2 指出：删除当前文件或删除数据字段指出的文件

响应 APDU



5）DEACTIVATE FILE（暂停文件）命令

DEACTIVATE FILE 命令暂停文件，该暂停是可逆的。在该命令成功完成后，除 SELECT 命令外，仅允许 ACTIVATE FILE、DELETE FILE、TERMINATE EF 和 DF 情况中的 TERMINATE DF 命令被执行。

如果一个 EF 被选择，则命令仅适用于该 EF，不适用于父辈 DF。

如果 P1-P2＝'0000'并且数据字段不存在，则该命令适用于已经被之前直接执行的命令选中的文件（即当前文件），P1-P2 的其他含义可参照 SELECT 命令，上述内容适用卡、管理命令中从“4）删除文件”到“8）终止文件”的命令。

DEACTIVATE FILE 命令的命令-响应对格式与 DELETE FILE 命令相同，INC＝'04'。

6）ACTIVATE FILE（激活文件）命令

ACTIVATE FILE 命令启动文件从下列状态到操作状态（激活的）的转变：创建状态，或初始化状态，或操作状态（暂停的）。

ACTIVATE FILE 命令的命令-响应对格式与 DELETE FILE 命令相似，INS＝'44'。

7）TERMINATE DF（终止 DF）命令

TERMINATE DF 命令终止当前选择的 DF 文件，该转变不可逆。命令成功完成后，DF 处于终止状态。

TERMINATE DF 命令的命令-响应对格式与 DELETE FILE 命令相同，INS＝'E6'。

8）TERMINATE EF（终止 EF）命令

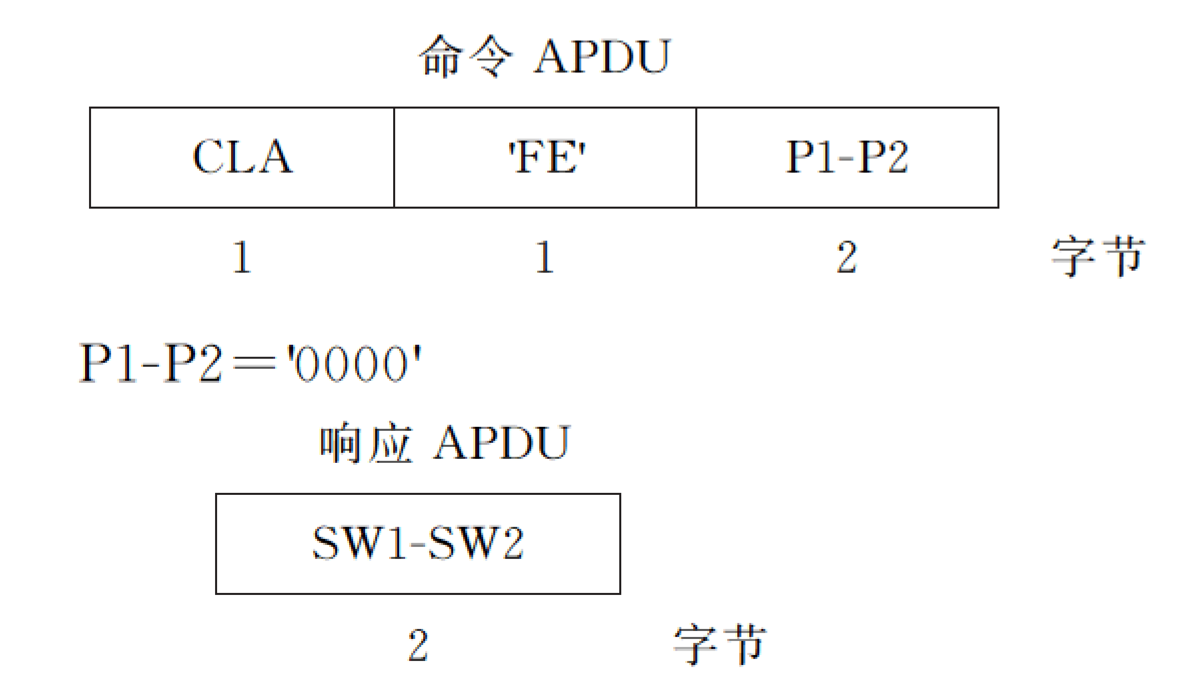
TERMINATE EF 命令将指定 EF 转变到终止状态，该转变不可逆。将被终止的 EF 应处于激活或暂停状态。

TERMINATE EF 命令的命令-响应对格式与 DELETE FILE 命令相同，INS＝'E8'。

9）TERMINATE CARD USAGE（终止卡使用）命令

TERMINATE CARD USAGE 命令将卡转变到终止状态，该转变不可逆。该命令的使用隐含选择 MF。对于支持该命令的卡，命令成功完成后，卡将不支持 SELECT 命令。

TERMINATE CARD USAGE 命令的命令-响应对如下。



命令 APDU

CLA	'FE'	P1-P2	
1	1	2	字节

P1-P2＝'0000'

响应 APDU

SW1-SW2	
2	字节

6.3.2 数据单元处理命令

1. 数据单元

在每个支持数据单元的透明结构 EF 内均有一个偏移值指向每个数据单元。从 0 对应 EF 的第一个数据单元开始，偏移每加 1 对应其下一个数据单元。偏移数据元采用二进制编码。

卡能够在历史字节及文件的文件控制信息中提供数据单元的大小(4 位或 8 位)，默认值为 8 位。

2. 通则

该组中每个命令可以使用短 EF 标识符或文件标识符。如果当命令发出时，要使用当前 EF，则当 P1-P2 设置为'0000'时，操作过程就可在该 EF 上完成。完成后，该标识的 EF 成为当前 EF。

INS P1 P2——该组所有命令应按以下方式使用 INS 的 b_1(b_1 为 0，即 INS 代码为偶数；b_1 为 1，即 INS 代码为奇数)。

(1) 如果 INS 的 b_1 为 0，P1 的 $b_8b_7b_6=000$，则 b_5 到 b_1 为 EF 的短标识符，并且 P2(所有 8 位)编码为 0～255 的偏移值，是将要读出的第一个数据单元的偏移值(从文件数据开始处算起)。

(2) 如果 INS 的 b_1 为 1，则，P1-P2 为文件标识符。P1-P2 设置为'0000'标识当前 EF。至少一个带有标记'54'的数据对象偏移应在命令数据字段中。出现在命令或响应数据字段中的数据应被封装进带有标记'53'或'73'的自由数据对象中。

该组命令中，SW1-SW2 设置为'63CX'，表示成功改变存储器状态，还有一个内部重试次数。$X>$'0'表示已重试次数，$X=$'0'表示未重试就完成命令功能。

3. 处理命令

1) READ BINARY(读二进制)命令

READ BINARY 命令的响应数据字段给出了支持数据单元的 EF 的(部分)内容。

命令 APDU

CLA	'B0'	P1-P2	Le	
1	1	2	1	字节

或

命令 APDU

CLA	'B1'	P1-P2	Lc	数据	Le	
1	1	2	0,1,3	0～N	0,1	字节

响应 APDU

数据	SW1-SW2	
0～N	2	字节

命令 APDU 和响应 APDU 中各字段的字节数的表达方式，对所有命令来说，都是一致的，因此后面不再标出字节数。

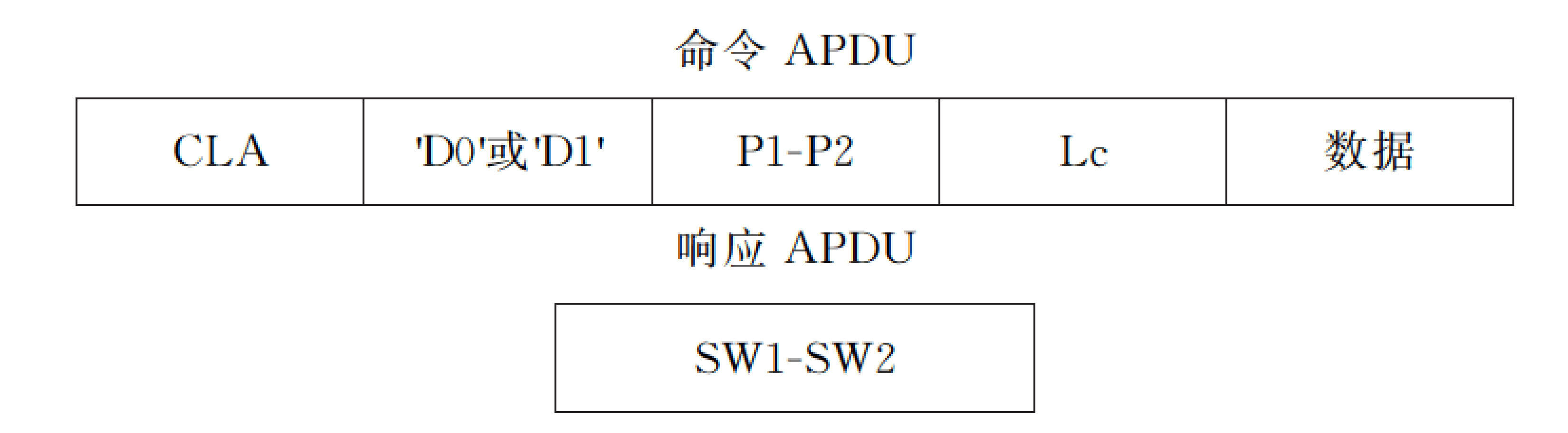
2）WRITE BINARY（写二进制）命令

WRITE BINARY 命令对 EF 文件执行下列写入操作之一。

（1）写入命令数据字段中指定的数据位（如果数据单元的字串不是在逻辑擦除状态下，则命令将失效，逻辑擦除状态由 ERASE BINARY 命令设置）。

（2）将命令数据字段中数据位和卡中已存在数据进行逻辑 OR 操作后写入。

（3）将命令数据字段中数据位和卡中已存在数据进行逻辑 AND 操作后写入。



命令 APDU

CLA	'D0'或'D1'	P1-P2	Lc	数据

响应 APDU

SW1-SW2

数据：要写入的数据单元串（INS＝'D0'），或偏移数据对象和要写入的封装成自定义数据对象的数据单元串（INS＝'D1'）

3）UPDATE BINARY（更新二进制）命令

UPDATE BINARY 命令执行用命令数据字段中数据位更新 EF 文件中已存在数据位的操作。当操作完成后，每个指定的数据单元的每一位将被更新为命令数据字段中的指定值。

命令 APDU 和响应 APDU 的格式与写二进制命令的格式相同，INS 为'D6'或'D7'。

4）SEARCH BINARY（搜索二进制）命令

SEARCH BINARY 命令执行在 EF 中搜索数据单元的操作，响应数据中返回找到的数据单元的偏移。当 Le 不存在或没找到匹配串时，响应数据字段不存在。

INS＝'A0'或'A1'

5）ERASE BINARY（擦除二进制）命令

ERASE BINARY 命令从一个指定偏移开始顺序设置 EF（部分）内容为逻辑擦除状态，但不删除内容，为 WRITE BINARY（写二进制）命令作准备。INS＝'0E'或'0F'。

6.3.3 记录处理命令

1. 记录

在每个支持记录的 EF 中,由一个记录号和(或)记录标识符来引用一个记录。

1) 由记录号引用

(1) 在每个支持线性结构的 EF 中,当增加或写入时,记录号应该按顺序分配,即按照创建的顺序。第一个记录(记录号为 1)是首先被创建的记录。

(2) 在每个支持循环结构的 EF 中,记录号应该依次按逆序分配,比如第一个记录(记录号为 1)是最近被创建的记录。

2) 由记录标识符引用

每个记录标识由应用提供。多个记录可以有相同的记录标识,在这种情况下,由记录中的数据或相对于当前记录的位置来区别不同的记录。如果记录的数据字段是一个 SIMPLE-TLV 数据对象,则记录标识是数据对象的第一个字节,即 SIMPLE-TLV 标记。

每一次由记录标识符引用,在命令中要指出目标记录相对于当前记录的位置:是第一个或最后一个出现的,是下一个或前一个出现的。

第一个出现的是带指定标识符在第一个位置的记录,最后出现的是带指定标识符在最后一个位置的记录。

下一个出现的应是带指定标识符的离当前记录最近,并且位置大于当前记录的记录;前一个出现的应是带指定标识的离该记录最近,并且位置要小于当前记录的记录。

2. 通则

P1——记录号或标识,'00'表示当前记录(擦除记录命令和增加记录命令除外)。

P2——短文件标识(1～30)和当前 EF。

该组命令中,SW1-SW2 设置为'63CX',表明存储器状态改变成功。在内部重试后,X>'0'表示已重试次数。X='0'表示没有重试。

3. 操作命令

1) READ RECORD(S)(读记录)命令

该命令响应数据字段给出 EF 文件中指定记录的(部分)内容(或一个记录的开始部分)。

命令 APDU

CLA	'B2'	P1-P2	Le

或

CLA	'B3'	P1-P2	Lc	数据	Le

响应 APDU

数据	SW1-SW2

如果 INS='B2',根据 Le 和记录的长度,可以表明读出的是一个记录或多个记录,而

且最后一个记录可能是完整的或不完整的。

如果 Le 指定的数据是记录长度的整数倍，则读出的最后一个记录是完整的，否则是不完整的（读出最后一个记录的开始部分）。

如果 INS='B3'，则命令读取由 P1 指定部分记录，命令数据字段包含一个数据对象的偏移（标记'54'），指向记录中读取的第一个字节。响应数据字段包含一个自定义数据对象（标记'53'）封装所读数据。

如果 Le 字段的内容为'00'，则命令完整读取请求的单个记录或记录序列（从 P1 到最后的所有记录）。

2） WRITE RECORD（写记录）命令

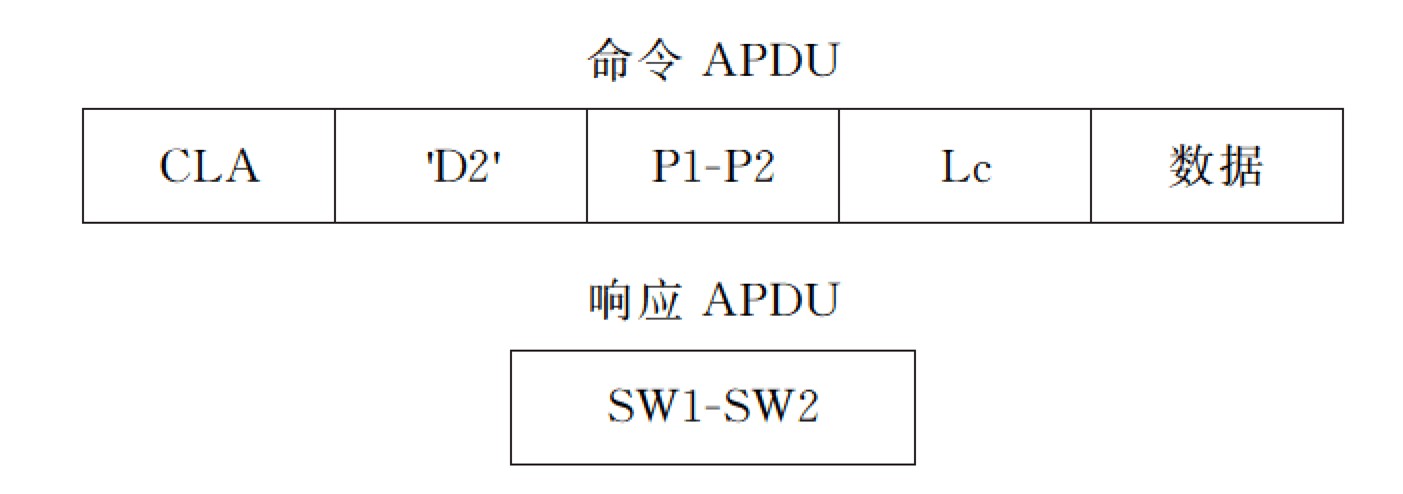
如果记录不处于逻辑可擦除状态，则命令中止。

WRITE RECORD 命令对 EF 文件执行下列操作。

（1） 按给定的命令数据字段中数据写入一个记录。

（2） 将给定的命令数据字段中数据和卡中已存在的数据按逻辑 OR 操作。

（3） 将给定的命令数据字段中数据和卡中已存在的数据按逻辑 AND 操作。



命令 APDU

CLA	'D2'	P1-P2	Lc	数据

响应 APDU

SW1-SW2

3） UPDATE RECORD（更新记录）命令

UPDATE RECORD 命令根据命令数据字段中给定的字节更新指定的记录。INS='DC'或'DD'。

4） APPEND RECORD（增加记录）命令

APPEND RECORD 命令在支持线性结构的 EF 文件结尾写入一个新的记录，或者在支持循环结构的 EF 中写入记录号为 1 的记录。当前记录指向成功增加的记录。

INS='E2'，新记录在命令 APDU 的数据字段给出。响应 APDU 的数据字段不存在。

5） SEARCH RECORD（搜索记录）命令

SEARCH RECORD 命令对 EF 中的记录进行搜索。待搜索的数据在命令的数据字段给出。响应数据字段给出了与搜索条件匹配的若干个记录号。命令完成后指向第一个匹配的记录为当前记录。

INS='A2'，如果没有搜索到匹配的记录，则响应的数据字段不存在。

6） ERASE RECORD(S) （擦除记录）命令

ERASE RECORD 命令设置 EF 中一个或多个记录为逻辑擦除状态，是由 P1 指定的记录或从 P1 开始直到文件结尾的连续记录序列。擦除记录并不删除记录，是为 WRITE RECORD 命令或 UPDATE RECORD 命令作准备。

INS='0C'，命令和响应的数据字段都不存在。

6.3.4 安全处理命令

1. 通则

该组命令保留 P1-P2 用于算法引用和一些相关数据引用(如密钥 key)等。如果有当前密钥和当前算法,则命令可以隐式地使用它们。

P1——除非特别指定,否则 P1 引用一个使用的算法:密码算法或生物识别算法。P1 设置为'00'表示不提供任何信息,即引用在发出命令前已经事先确定,或者由命令数据字段提供。

P2——除非特别指定,否则 P2 设置为 '00' 表示不提供任何引用信息,即在命令发出前已限定引用或由命令数据字段提供,或者是 password 编号、密钥编号或一个短文件标识。

该组命令中,SW1-SW2 设置为'6300'或'63CX'表示验证失败。$X>$'0'表示重试次数。SW1-SW2 设置为'6A88'表示引用数据没有找到。

在后面的响应 APDU 中,如果仅有 SW1-SW2(不存在数据字段),则不再表示出。

2. 操作命令

1) INTERNAL AUTHENTICATE(内部鉴别)命令

INTERNAL AUTHENTICATE 命令利用读写器发来的口令数据和存储在卡中的秘密(如密钥)计算卡鉴别数据。

命令 APDU

CLA	'88'	P1-P2	Lc	数据	Le

数据:鉴别相关数据(如口令)

响应 APDU

数据	SW1-SW2

数据:鉴别相关数据(如对口令的应答)

(1) 如果相关秘密属于 MF,则命令将卡作为整体鉴别。

(2) 如果相关秘密属于 DF,则命令将鉴别该 DF。

任何鉴别可能在先前的命令(如 VERIFY、SELECT)或选择(如相关秘密)执行完毕后才能成功完成。

为了限制将来的相关秘密和算法的使用,卡能够记录命令执行的次数。

注意:响应数据字段可以包含进一步的安全功能使用的数据(如随机数)。

2) GET CHALLENGE(取口令)命令

GET CHALLENGE 命令要求获取口令(如用于密码鉴别的随机数或用于生物特征鉴别的一段提示语句)用于安全相关过程。该口令至少在下一个命令(如 EXTERNAL AUTHENTICATE 命令)有效,没有其他特定条件。

命令 APDU

CLA	'84'	P1-P2	Le

响应 APDU

数据	SW1-SW2

数据：口令

3）EXTERNAL AUTHENTICATE(外部鉴别)命令

EXTERNAL AUTHENTICATE 命令根据卡的计算结果(是或否)有条件地更新安全状态，该结果基于先前由读写器发出的口令(如 GET CHALLENGE 命令)，一个存储在卡中的密钥或秘密，以及由读写器传输的鉴别数据共同计算得出。

命令 APDU

CLA	'82'	P1-P2	Lc	数据

Lc： 不存在或存在

数据：不存在或鉴别相关数据(口令的响应)

任何成功的鉴别要求使用最后从卡中获取的口令。卡将记录不成功的鉴别(如限制引用数据的使用次数等)。

若不存在命令数据字段，可用于得到可进一步重试的次数'X'(SW1-SW2 设置为'63CX')，或不要求验证(SW1-SW2 设置为'9000')。

上述 3 条命令(取口令、内部鉴别、外部鉴别)的执行过程可参考第 5 章。

4）VERIFY(验证)命令

VERIFY 命令对卡中存储的引用数据(如 password)或传感信息(如指纹)和读写器发送的验证数据进行比较。比较成功后将更新安全状态。否则卡将记录不成功的比较次数(将限制进一步引用数据的使用次数)。

命令 APDU

CLA	'20'或'21'	P1-P2	Lc	数据

P1＝'00'　　P2 见安全处理命令的通则

数据内容如下。

(1) 如果 INS＝'20'，命令数据字段通常为验证数据。若命令数据字段不存在，则用于检查之前 VERIFY 命令执行情况：SW1-SW2＝'63CX'，其中'X'表示重试次数，或 SW1-SW2＝'9000'。

(2) 如果 INS＝'21'，命令数据字段应为验证数据对象，通常是存在的。

5）CHANGE REFERENCE DATA(替换引用数据)命令

CHANGE REFERENCE DATA 命令利用读写器发送来的新的引用数据替换保存在卡中的引用数据；或者将卡中的引用数据同读写器发送的验证数据进行比较，并利用读写器发送的新的引用数据有条件地替换原有数据。INS＝'24'。

6）ENABLE VERIFICATION REQUIREMENT(允许验证要求)命令

ENABLE VERIFICATION REQUIREMENT 命令打开要求比较引用数据和验证数据的开关。INS＝'28'。

7) DISABLE VERIFICATION REQUIREMENT(禁止验证要求)命令

DISABLE VERIFICATION REQUIREMENT 命令关闭要求比较引用数据和验证数据的开关。INS='26'。

8) RESET RETRY COUNTER(复位重试计数器)命令

RESET RETRY COUNTER 命令复位引用数据重试次数为初始值,或者完成复位引用数据重试次数为初始值并改变引用数据。

9) PERFORM SECURITY OPERATION(完成安全操作)命令

PERFORM SECURITY OPERATION 命令完成下列操作。

(1) 密码校验和的计算。

(2) 数字签名的计算。

(3) 哈希代码的计算。

(4) 密码校验和的验证。

(5) 数字签名的验证。

(6) 证书的验证。

(7) 加密。

(8) 解密。

上述安全操作使用同一 INS 编码'2A',而由 P1 和 P2 中的参数来确定具体操作的内容。

命令 APDU

CLA	'2A'	P1-P2	Lc	数据	Le

8 种操作的命令 APDU 和响应数据字段如表 6.8 所示。

表 6.8 8 种安全操作的命令 APDU 和响应数据

命　　令	INS	P1	P2	命令数据	响应数据
(1) 密码校验和的计算	2A	8E	80	存在	密码校验和
(2) 数字签名的计算	2A	9E	9A、AC	存在	数字签名
(3) 哈希代码的计算	2A	90	80 或 A0	存在	哈希代码或不存在
(4) 密码校验和的验证	2A	00	A2	存在	不存在
(5) 数字签名的验证	2A	00	A8	存在	不存在
(6) 证书验证	2A	00	92、AE	存在	不存在
(7) 加密	2A	82	80	被加密的数据	加密的数据
(8) 解密	2A	80	82	被解密的数据	解密的数据

说明:① 上述 8 条命令的 P1-P2 可在表 6.6 中查到(模板标记'7D'),命令数据都存在。

② P1-P2 具有唯一性,可确定执行哪一条命令。

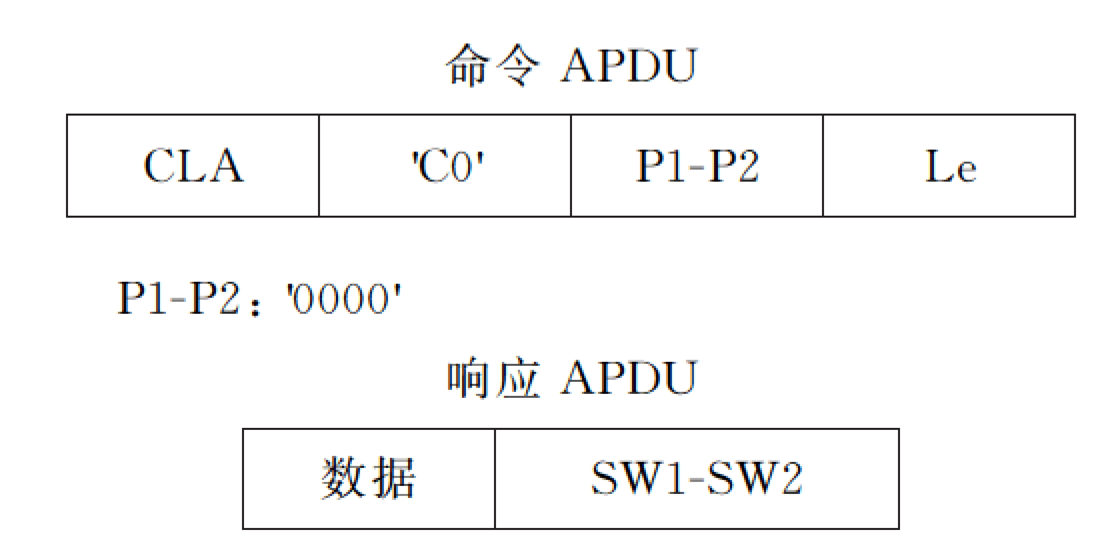
③ 在密码学中已制定了多种标准实现上述命令(在本书第 5 章中已讨论了 DES 算

法、RSA 算法和哈希算法等)，在卡内由微处理器和操作系统完成，某些命令的操作很复杂。

6.3.5　传输处理命令

GET RESPONSE(获取响应)命令发送在上一条命令的响应 APDU 中未能发送的部分数据。

如果 Le 字段包含'00'字节，则所有可用字节应被返回。对于短 Le 字段长度限制为 256B，对于长 Le 字段长度限制为 65 536B。



命令 APDU

CLA	'C0'	P1-P2	Le

P1-P2：'0000'

响应 APDU

数据	SW1-SW2

数据：有错误则不存在，或根据 Le 的部分数据

6.3.6　多应用环境的应用管理命令

1. 生命周期状态

多应用环境中的卡应用管理可以通过 SELECT 命令以应用标识符 AID 为 DF 名称进行选择。

图 6.4 所示为卡的应用生命周期。它有 4 种状态：初始化、创建、操作激活和操作暂停。状态的转换通过以下 3 条应用管理命令实现。

- 应用管理请求(APPLICATION MANAGMENT REQUEST)命令。
- 加载应用(LOAD APPLICATION)命令。
- 删除应用(REMOVE APPLICATION)命令。

图 6.4 中的激活文件是用 ACTIVATE FILE 命令实现的，暂停文件是用 DEACTIVAEE FILE 命令实现的(见 6.3.1 节)。对图说明如下。

(1) 在应用生命周期的 4 种状态中，操作激活状态是一定存在过的，其他 3 种状态是可选的。

(2) 状态的转换有以下两种方式。

① 顺序执行两条命令才能转换，如从“应用不存在”转到“操作激活状态”需要顺序执行应用管理请求(P1＝'0E')命令和加载应用命令。

② 执行一条命令即可实现状态转换，如删除应用(P1＝'07')命令。为了理解应用生命周期图，首先需要理解下面介绍的命令功能。

2. 应用管理命令

(1) APPLICATION MANAGEMENT REQUEST(应用管理请求)命令。

APPLICATION MANAGEMENT REQUEST 命令实现生命周期中状态转换的请求。

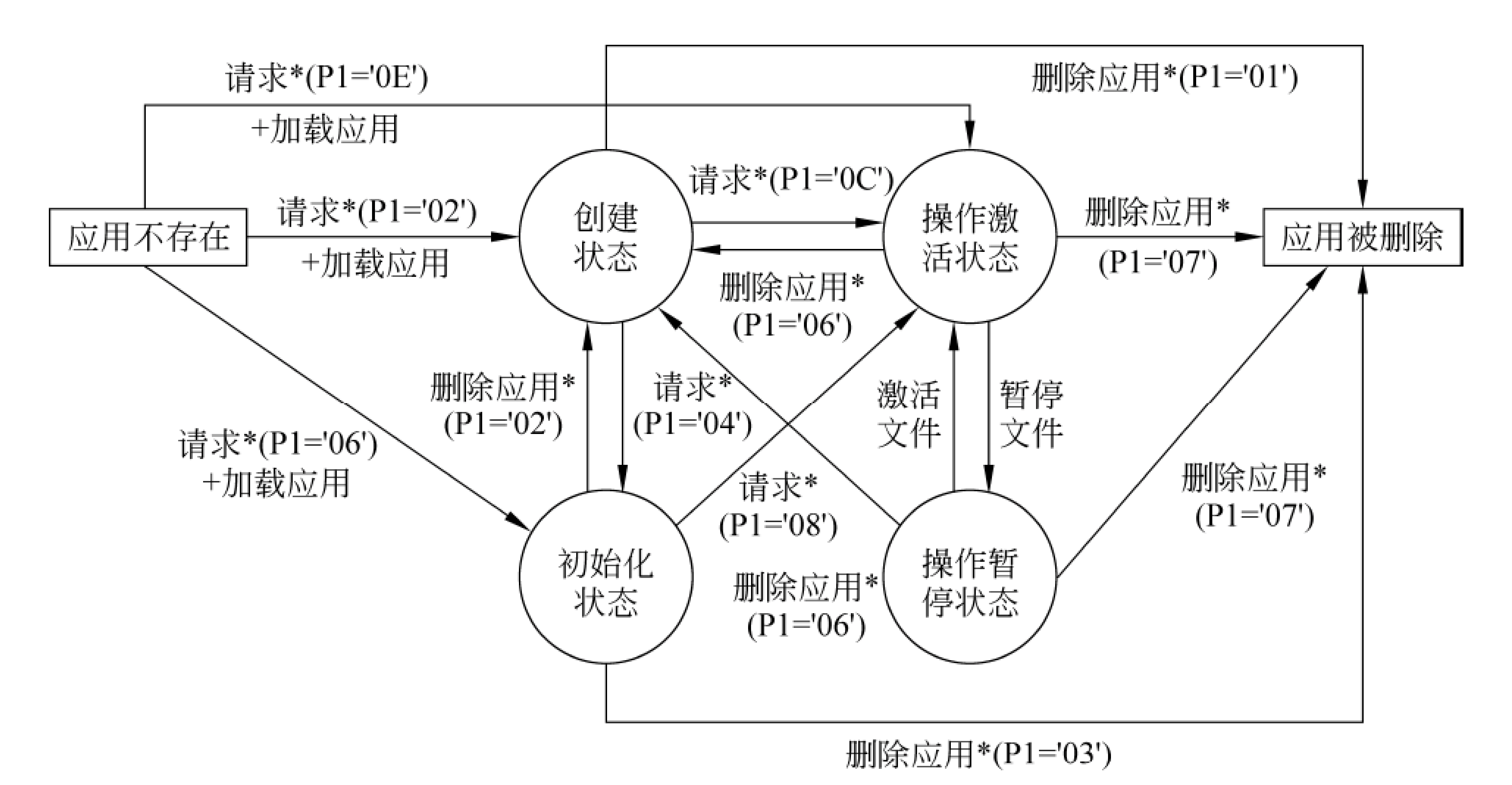


图 6.4　卡的应用生命周期

命令 APDU

CLA	'40'或'41'	P1-P2	Lc	数据	Le

P1：应用生命周期状态控制，在图 6.4 中，根据 P1 值转移到相应状态

P2：提交成验证应用管理请求

数据：目标应用的 AID(标记'4F')，必选

可选的数据有：

存储资源分析(标记'7F65')

数字签名模板(标记'7F3D')，包含数字签名 DO(标记'9E')等

其他：标记为'42'、'51'、'53'或'73'等(含义见表 3.2)

Le：可能不存在，即响应 APDU 的数据可能不存在

(2) LOAD APPLICATION(加载应用)命令。

LOAD APPLICATION 命令将应用数据传送到卡。

命令 APDU

CLA	'EA'或'EB'	P1-P2	Lc	数据	Le

P1-P2：指出数据的含义，如偏移值或序列号等

数据：应用组件(建立某一应用所需的其他数据)

Le：可能不存在

执行上述两条命令后，将建立某一应用所需的应用数据和安全信息等传送到卡，并实现状态的转换。

(3) REMOVE APPLICATION(删除应用)命令。

INS='EC'或'ED'

REMOVE APPLICATION 命令删除一个应用，并可能收回分配给该应用的存储资

源;或者从初始化状态、操作(激活和暂停)状态转到创建状态。

命令 APDU

CLA	'EC'或'ED'	P1-P2	Lc	数据	Le

P1:根据图 6.4 删除应用

P2:'00'

数据:不存在,或要删除的卡管理应用的信息(ISN='EC');或目标应用的 AID(标记'4F')、数字签名(标记'7F30'、'9E')等(INS='ED')

Le:可能不存在

在图 6.4 中,根据 P1 值转移到相应状态。

本章定义的命令适用范围如下。

在 ISO/IEC 7816 中定义的命令是根据应用需要陆续推出的,此时可能会对前面提出的命令细节进行一些更改。在早期的智能卡中,有相当多的命令是由应用提供者或设计者创建的。智能卡应用范围很广,繁简不同,各类应用在卡中采用的命令系统也不相同。

本章介绍的命令系统可以使用在接触式、非接触式智能卡和 RFID 标签中,逻辑加密卡中不采用类似的命令系统。

习题

1. 请说明命令 APDU 的结构。其中哪些内容是必须有的?
2. 响应 APDU 包含哪些内容?当命令正确执行时返回什么状态字节(SW1-SW2)?
3. 今有一条读二进制命令,如果选用通道 3 传送数据,并且采用安全报文传输,请写出该命令 APDU 各字段的编码。
4. 在命令-响应对中,N_e 和 N_r 各表示什么意义?
5. 本章中提到的命令链有什么意义?在什么情况下要执行命令链?如何实现?
6. 在 ISO/IEC 7816 中所讲的命令是否就是智能卡中的微处理器指令?如果不同,请说明它们的主要区别。
7. 写二进制命令可执行哪几种操作?为什么处于逻辑擦除状态的存储区才能执行写命令?
8. 读二进制命令和读记录命令各对哪些 EF 结构起作用?如文件结构不满足要求,将发生什么情况?
9. 在本书中,有哪些命令主要是为了安全或相互鉴别而引入的?在实际应用时,为了满足符合国际标准的要求,所有公司所确定的命令是否应该完全一致?
10. GET CHALLENGE 命令的主要作用是什么?
11. 哪些命令用于验证持卡人的身份?哪些命令用于 IC 卡和读写器之间的鉴别?
12. 在复位应答之后,IC 卡与读写设备之间是怎样配合工作的?是否 IC 卡和读写器都有可能发命令?

13. IC 卡接收到读写器发来的命令后，如何实现命令所规定的功能？

14. 历史字节中包含哪些内容？已知我国的国家编码为 156，请问在历史字节中如何用 TLV 数据对象表示？

15. 通过本章的学习，你对-TLV 定义的 3 种类别（通用类、应用类和上下文相关类）的使用场合、唯一性有什么认识？请举例说出上下文相关类（模板标记为'6x'和'7D'）中的某一标识的使用情况。

16. 智能卡的命令系统和计算机的指令系统有什么区别？

第 7 章　IC 卡芯片和卡内操作系统

IC 卡按其所装配的芯片不同而分成逻辑加密卡和智能卡(或称为 CPU 卡)。本章主要论述适合 IC 卡使用的逻辑加密芯片和 CPU(内含 COS)芯片。

7.1　IC 卡的逻辑加密芯片

逻辑加密卡主要是由 E^2PROM 单元阵列和密码控制逻辑构成的,具有一定的保密逻辑功能,但不像 CPU 卡那样能进行复杂的密码计算。因此适用于一些需要保密功能,但是对保密功能要求又不是很高的应用场合。

下面介绍 Atmel 公司和 Siemens 公司的接触式 IC 卡和 Philips 公司的非接触式 IC 卡。

7.1.1　名词解释

在具体分析之前,需要对本章中经常使用的术语进行解释,以便读者理解。

1. E^2PROM 的写入和擦除

写入是指往芯片内的存储区写入数据 0 的操作。芯片的存储器由 E^2PROM 构成,而 E^2PROM 有其特有的读写机制,写入就是指写 0 的操作。写入前必须先进行擦除,然后写入。

擦除是指往芯片内的存储区写入数据 1 的操作。芯片的存储器由 E^2PROM 构成,而 E^2PROM 有其特有的读写机制,擦除就是写 1 的操作。需要特别指出的是,擦除操作是按行进行的,对一行的任意一位进行擦除操作,其结果是擦除整行,而写入可按位进行。

E^2PROM 的写入和擦除时间为几毫秒。

2. 熔断

对于物理的熔丝而言,是指用外加大电流将芯片内熔丝烧断的过程。如果用 E^2PROM 单元来表示一种熔丝信号,熔断是指对该单元进行了一次写入操作。即该单元为 1 时表示它代表的熔丝未熔断,该单元为 0 时表示熔丝熔断了。需要指出的是,用 E^2PROM 表示的熔丝信号与真正的物理熔丝是不同的,后者烧断后是不能再接通的,而前者有可能通过擦除恢复成 1,是否可恢复,由设计者决定。

3. 个人化

E^2PROM 中的存储单元按其所起的作用不同而分成若干个区。个人化是指 IC 卡由发行商发行给个人的过程。在这个过程中,由发行商按要求往 E^2PROM 中写入发行商代码、用户密码及用户身份标识等。

4. 密码错误计数

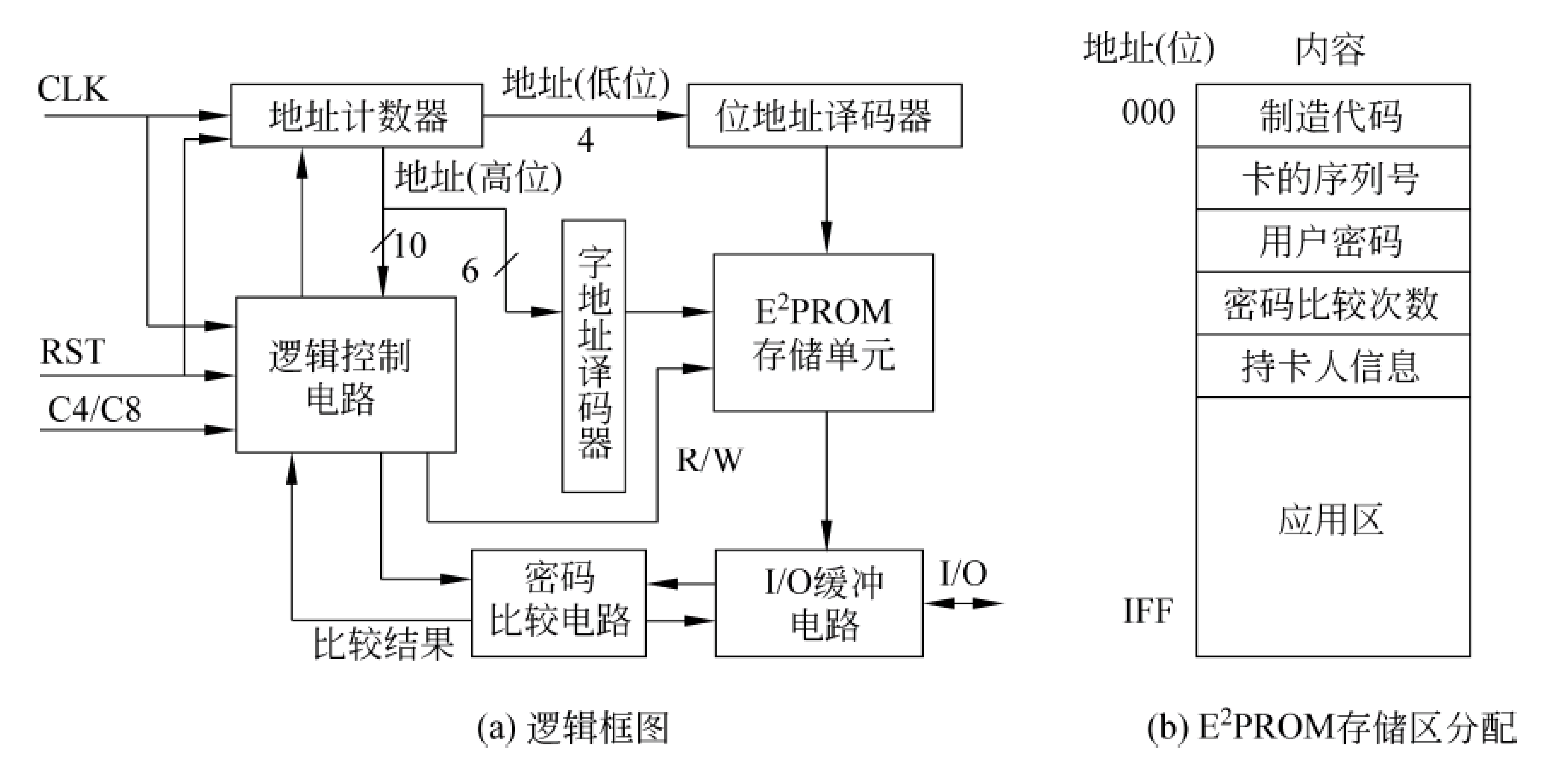
用户使用逻辑加密卡时,首先输入用户密码。在卡中设置有用户密码比较计数区。设置该区的目的是防止人为地对密码进行猜测,用该区来累计不正确的密码输入比较次数。当连续 N 次密码比较均不正确后,卡将自锁,拒绝以后的任何操作。用户只能将卡交给发

行商，由发行商读出卡中的应用区数据（如余额），并重新发售另一张卡使用，有的卡可用发行商专设的解锁密码，由发行商对卡解锁。设置的密码比较次数 N 要折中考虑：一方面要使猜测成功的可能性小，尽可能减小 N；另一方面又要考虑到用户操作的失误，N 的值又不能太小。实践证明，当采用 16 位二进制用户密码时，$N=4$ 是比较合理的设置。

7.1.2 逻辑加密卡功能和芯片举例

1. 逻辑框图

逻辑加密卡芯片从功能上看，主要分为两个部分：一部分是 E^2PROM 存储单元；另一部分是数字控制电路，如图 7.1 所示（举例）。图中，CLK、RST 和 I/O 端口信号的要求应符合 ISO/IEC 7816 的规定（见本书第 4 章）。



(a) 逻辑框图　　(b) E^2PROM存储区分配

图 7.1 逻辑加密卡框图（举例）

在逻辑加密卡中，为完成读写操作，由设计者自行定义 C_4 和 C_8 触点的功能。

在图 7.1 中，假设 E^2PROM 的存储容量为 1Kb（64 字，每个字 16 位），地址计数器的长度为 10 位，其中低位地址（4 位）送到位地址译码器，高位地址（6 位）送到字地址译码器，在读/写（R/W）的控制下，对 E^2PROM 中某位进行读/写。

逻辑控制电路和密码比较电路等，根据设计要求，对 E^2PROM 各个存储区的读出、写入、擦除和工作流程进行控制。

地址计数器只有计数功能，不能从外界接收地址，当加电或 RST 信号来时清 0，所以对 E^2PROM 只能按照地址顺序访问，当卡加电运行时，在读写器送来的操作命令和卡内逻辑电路的控制下，地址计数器自动完成计数功能（按位寻址）。

2. E^2PROM 存储区域分配（举例）

逻辑加密卡一般具有如下的存储分区，如图 7.1(b)所示。

(1) 制造代号区。制造代号区由制造厂商写入，用于记录卡片的制造信息，以便于以后验证卡的出处。

(2) 发行代号区。发行代号区用于记录卡片的发行信息，如卡的序列号。

(3) 用户密码区。当卡片个人化完成后，由该密码保护卡内的应用区域。使用时由用户输入用户密码，只有密码比较正确后，才允许对应用区进行读写操作和修改密码

操作。

(4) 密码比较计数区。出于安全保护的目的,防止人为对密码进行猜测,需要限制密码比较次数。

(5) 个人区。个人区记载用户的个人身份标识。写入和擦除受密码保护,但可以自由读出,以核实用户身份。

(6) 应用区。应用区内一般存放与消费有关的数据(钱),由于逻辑加密卡没有加/减法计算功能,因此用户的每次消费额不是任意的,一般将应用区的每一位代表一定的金额(假设为 A),若应用区有 256 位,则可在卡内存入金额 256×A,此时将应用区改写成全1,然后消费 1 次,将应用区中的 1 位由 1 改写为 0。当应用区全部为 0 时,表示卡内存款已全部用完,卡将作废或重新充值。

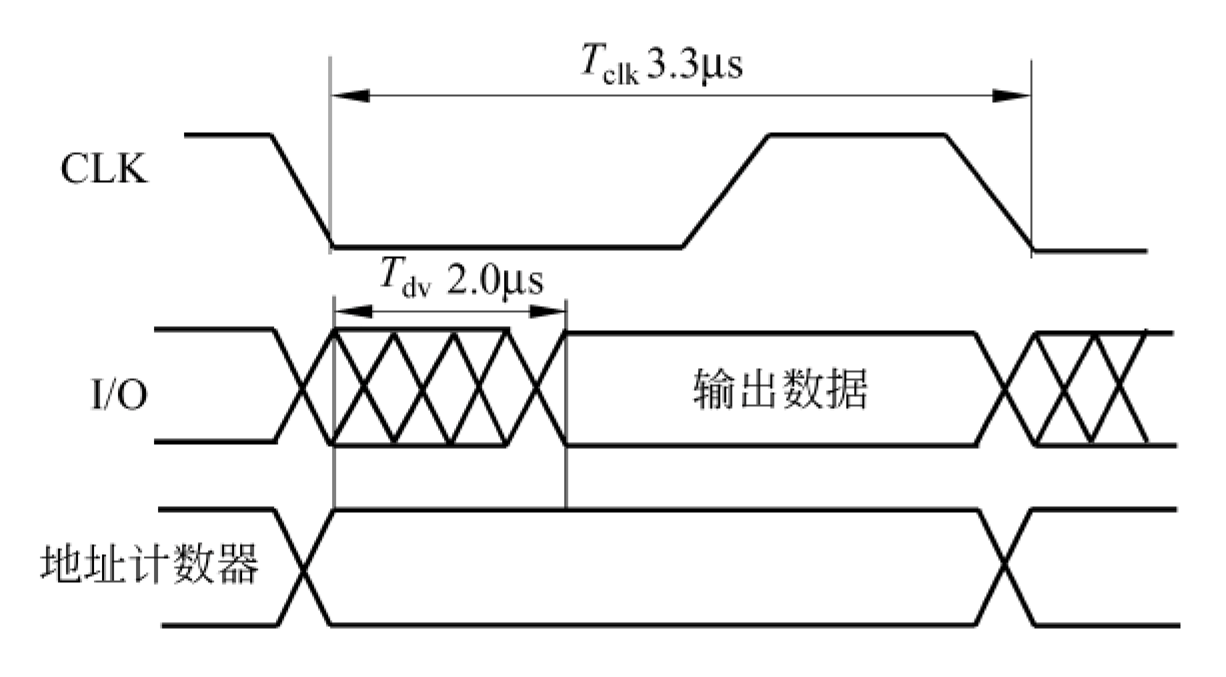
3. 公司产品

1) 美国 Atmel 公司

美国 Atmel 公司将 C8 触点定义为编程信号 PGM,用以通知芯片进行写入和擦除操作。由 PGM、RST、CLK 信号和内部地址计数器决定了 4 种操作模式(命令),如图 7.2 所示。有总清 RST、密码比较 CMP、读 READ、写 WRITE 4 条命令,后 3 条命令的操作时序如图 7.3~图 7.5 所示。在这 4 种操作命令中,输出的控制在卡内完成。如果读出的条件不满足,则在 I/O 线上出现的数据无效(Z 状态)。CMP 操作只在用户密码地址区进行,是通过内部地址计数器来控制的。

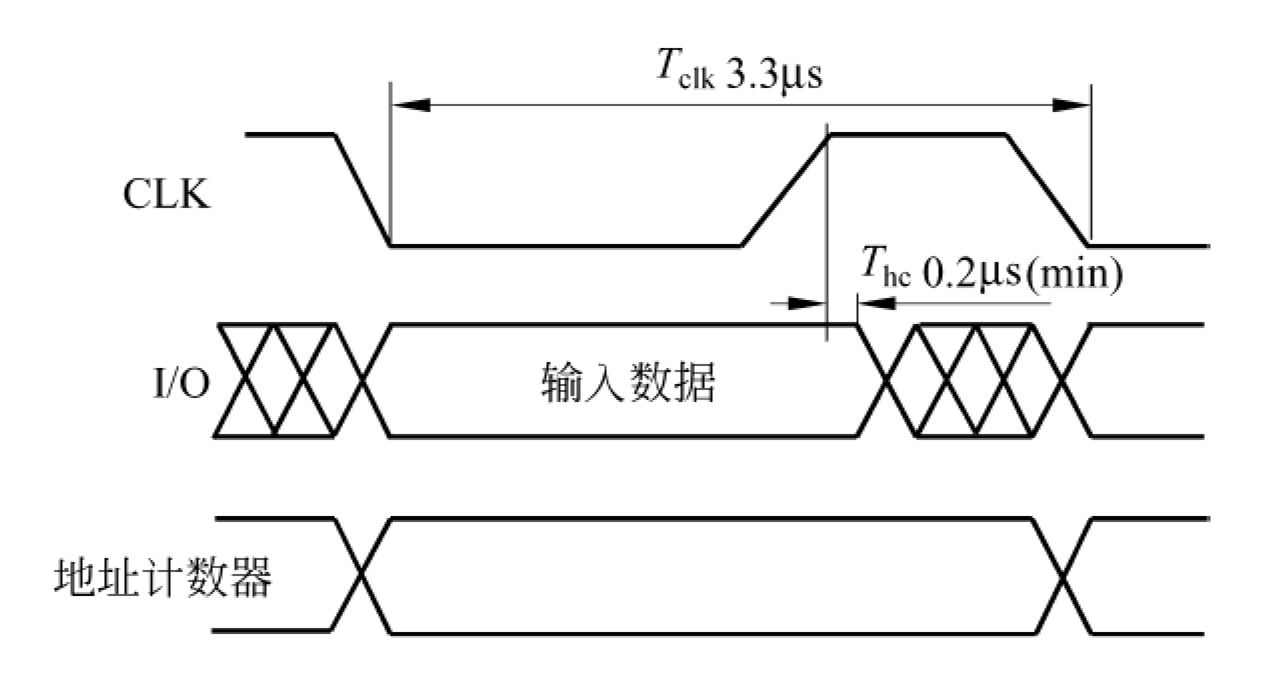
命令名	PGM	RST	CLK	描　述
RESET(RST)	X		0	卡内地址计数器(在 RST 的下降沿)清 0。当 RST 和 CLK 信号都为 0 时,存储器内的数据开始出现在 I/O 线上
READ (INC/READ)	0	0		卡内地址计数器(在时钟下降沿)加 1,存储器内的数据输出在 I/O 线上(图 7.3)
CMP(INC/CMP)	0	0		外部输入数据与卡内密码进行比较(图 7.4)。当 CLK 为低时,输入 I/O 线上必须稳定。地址计数器在时钟下降沿加 1
WRITE	1	0		在时钟上升沿前,I/O 数据必须准备好,然后 CLK 必须保持为高至少 5ms 时间,等待写入操作完成(图 7.5)。随后,在时钟下降沿,刚写入的数据出现在 I/O 线上,以被验证。在这个时钟下降沿地址计数器不加 1
VERIFY	0	0		

图 7.2　AT88SC102 的操作模式



注：T_{clk}为时钟周期。在 CLK 的下降沿，计数器加 1。存储器内的数据经过一段延时 T_{dv} 以后，读出在 I/O 线上。在这个时序中包含了地址加 1(INC)和读出(READ)两种操作

图 7.3　读时序



注：在 CLK 下降沿，地址计数器加 1，这时外部开始输入待比较的数据。在 CLK 上升沿，I/O 上的数据被锁存，I/O 线上的数据在 CLK 上升沿后至少保持 T_{hc}时间。当下一个 CLK 下降沿来临时，执行这次比较操作，同时地址计数器加 1

图 7.4　比较时序

READ　PROGRAM　VERIFY

CLK

T_{chp} 5.0ms(min)

T_{dv} 2.0μs(max)　T_{ds} 0.2μs(min)

I/O　有效输入数据

PGM　T_{spr} 2.2μs(min)

地址计数器

注：在 CLK 上升沿到来之前(T_{spr}时间)，PGM 应升为 1，I/O 上由外部给出写入数据(提前 T_{ds}时间)。当 CLK 为 1 时，开始执行写 0 或写 1 操作，这时 CLK 应至少保持 5ms 时间为 1(T_{chp})。在紧接着的是 CLK 下降沿，地址计数器不发生变化，I/O 上出现存储器输出的数据，提供给外部验证上次写操作是否成功

图 7.5　写(编程 PROGRAM)时序(包含写后验证 VERIFY)

2）SIEMENS 的逻辑加密卡芯片 SLE 4432/4442

SLE 4432/4442 内含 256×8 位 E^2PROM 存储器和 32×1 位保护存储器，该保护存储器对 E^2PROM 的前 32 字节（第 0～31 字节）进行写/擦除保护。保护位的设置是一次性的，不能修改。

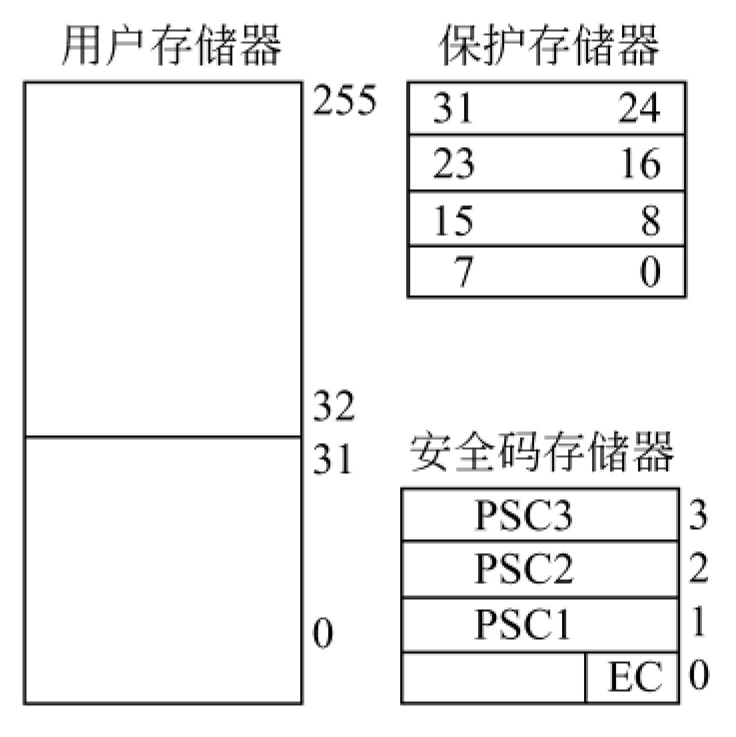


图 7.6　SLE 4442 存储器分配

SLE 4442 还有一个可编程安全码（PSC）逻辑，整个存储器除了 PSC 以外，均可读，而且只有在比较 PSC 正确后才能进行写/擦除操作。在 3 次比较 PSC 不正确后（在 EC 中存放比较次数），将锁住后续的 PSC 比较及写/擦除操作。

SLE 4442 的存储器分配如图 7.6 所示。

SLE 4432 除了不具备安全码存储器外，其余均与 SLE 4442 相同。

用户存储器可以按字节擦除和写入，擦除时，数字字节的 8 位被置成 1；写入时，E^2PROM 中的信息与输入数据比较后，逐位写成 0。

3）荷兰 Philips 的非接触式 IC 卡 Mifare

Philips 是世界上最早研制非接触式 IC 卡的公司。其早期产品系列有 Mifare Standard（逻辑加密卡，E^2PROM 容量为 8K 位）、Mifare Light（逻辑加密卡，E^2PROM 容量为 384bit）、Mifare PLUS（第一代双界面微处理器卡）、Mifare PRO 和 Mifare PROX（第二代双界面微处理器卡）。

Mifare 技术的发展状况如图 7.7 所示。

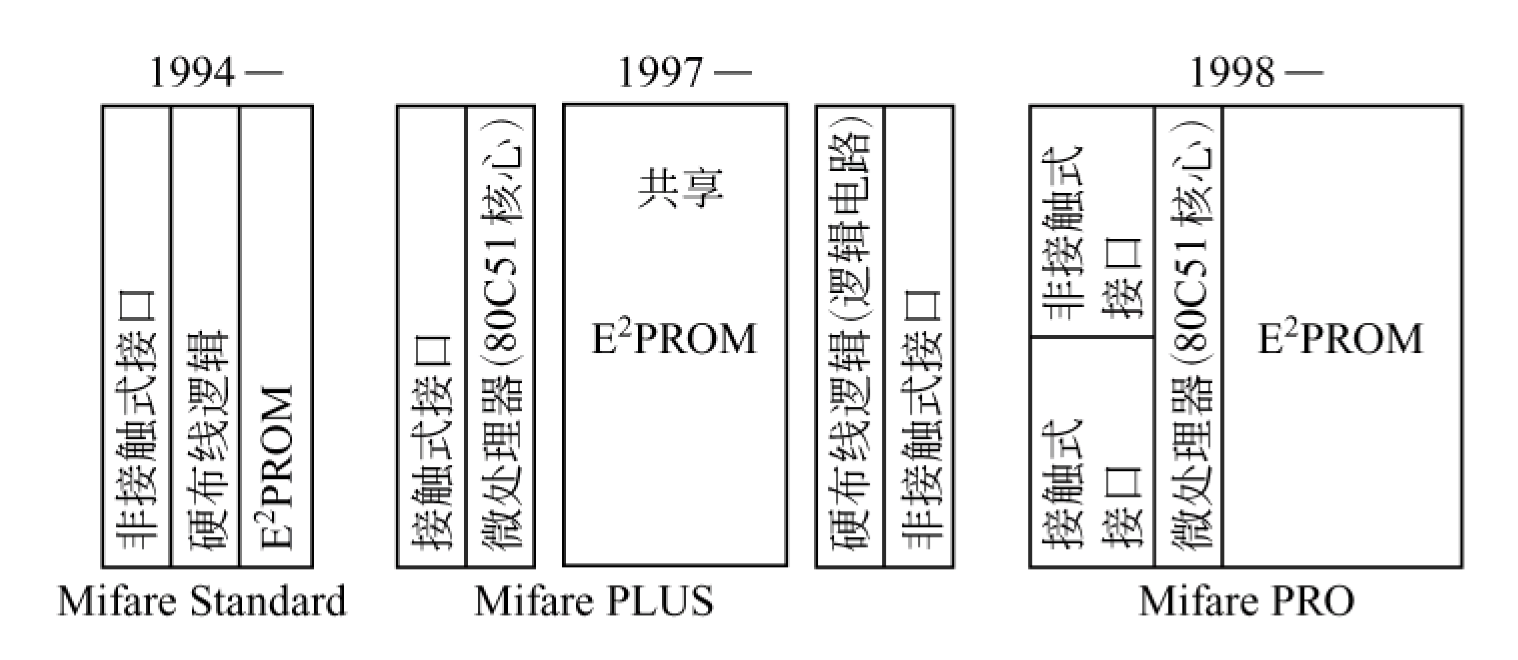


图 7.7　Mifare 技术的发展

图 7.7 中，非接触式接口符合 ISO/IEC 14443 Type A 标准（见第 9 章），接触式接口符合 ISO/IEC 7816 标准。非接触式 IC 卡已是智能卡（CPU 卡）。

Mifare PLUS 和 Mifare PRO 为双界面卡，既可用作接触式卡，也可用作非接触式卡。Mifare PLUS 的接触式界面有微处理器支持，非接触式界面仅有逻辑电路支持，但芯片内的 E^2PROM 为两者共享。Mifare PRO 的两个界面共享微处理器和 E^2PROM。

7.2 移动通信中的 SIM 卡

7.2.1 SIM 卡概述

以微处理器为基础的智能卡在移动通信领域中的应用可以追溯到 20 世纪 80 年代初期，当时欧洲有些国家讨论要在模拟移动通信网中采用 IC 卡。而此时，欧洲正在讨论建立新的数字移动通信标准，以便为用户提供国际漫游。因此，在新的数字移动通信系统中采用 IC 卡技术，很自然地被列入了新数字移动通信系统（即全球移动通信 GSM 系统）的技术标准中，并将这种 IC 卡称为用户识别模块（Subcrible Identity Module，也称 SIM 卡）。

全球移动通信（Global System for Mobile，GSM）系统中的用户识别模块（SIM 卡）是一种带微处理器的封装在塑料片上的 IC 卡，它符合 IC 卡国际标准 ISO/IEC 7816 要求。它是 GSM 系统中移动终端（手机＋SIM 卡）的重要组成部分，是用户进网登记的凭证。手机与 SIM 卡分工明确，如果 SIM 卡已插入手机，打电话时，通过 SIM 卡进行鉴权后，手机才有可能接通移动通信网络。手机进入 2G 时代。

有 3 种功能相同而形式不同的 SIM 卡投入使用：一种是卡片式 SIM 卡，尺寸为 85.6mm×53.98mm×0.76mm，符合接触式 IC 卡的 ISO/IEC 7816 标准；另一种形式是嵌入式 SIM 卡，尺寸为 25mm×15mm×0.8mm，称为 Micro SIM 卡；还有一种卡，尺寸为 12.3mm×8.8mm×0.7mm，称为 Nano SIM 卡。

中国移动通信大运营商有 3 家：中国移动、中国联通和中国电信。进入 3G 时代，3 家通信运营商被指定运行的移动网络通信的制式如下：中国联通为 WCDMA（源自欧洲）；中国移动为 TD-SCDMA（源自美国）；中国电信为 CDMA2000（是中国大唐电信公司自主研发的通信协议）。目前全球应用最广泛的制式为 WCDMA。

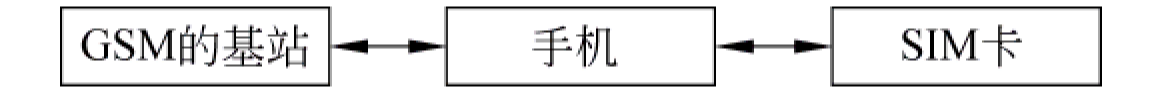
有关移动通信网的内容及手机的应用将在 13.4 节中论述。

下面介绍的是 SIM 卡的基本原理，具体情况与生产厂家有关，且在不断改进。

7.2.2 SIM 卡的结构和工作原理

1. SIM 卡的基本结构和使用流程

SIM 卡和手机、GSM 基站的连接关系如下。



用户从苹果、三星或华为等公司购置手机后，向移动通信运营商申请移动电话号码和 SIM 卡。电话号码随卡不随机，通话费等也记录在 SIM 卡中用户账单上。

手机与基站之间为无线连接。SIM 卡通过卡上的 I/O 触点与手机传送信息。SIM 卡的硬件由五部分组成：微处理器、ROM、RAM、E^2PROM 和串行通信单元，而且集成在一个芯片中。E^2PROM 的存储容量有 8KB、16KB、32KB、64KB、512KB、1MB 等多种，如果采用 8KB，则可存储 100 组电话号码及其对应姓名，15 组短信，25 组最近拨出的电话

号码和 4 位 PIN。

卡内操作系统(COS)存放在 ROM 中,每次用户使用手机时,首先由 GSM 基站对手机进行鉴别(称为鉴权),如果通过鉴别,则由使用人输入 PIN,以验证使用人的身份合法性,然后在使用人的操作下实现使用目标,GSM 网络与 SIM 卡之间传送的命令和数据都要进行加密。

每次加电开机后要输入 PIN 才能使用,连续输入 3 次错误 PIN 码,SIM 卡被锁住,此时需用解锁码 PUK(8 位)将 SIM 卡解锁,PUK 使用 10 次后,SIM 卡将被作废。SIM 卡个人化时输入的 PIN 码为 1234 或 0000。

手机包括以下内容:CPU、存储器(Flash RAM)、I/O 设备(显示屏、虚拟键盘、USB 接口、射频空中接口及与 SIM 卡之间的串行接口)等。

手机内有 CPU 核、DSP 核(数字信号处理器)、通信协议处理单元(通过空中接口协议软件,完成空中接口与基站的通信功能,实现语音和数据的传送)等。

如果在 SIM 卡中安装的 E^2PROM 超过 512KB,该卡称为 STK 卡,增加了一些服务项目,其中某些项目是要收费的。

为使 SIM 卡能正常工作,其各触点的电性能及电源开/关时的电性能都是有所要求的。当电源开启时,SIM 卡可处于两种方式,即工作方式和休闲方式。在工作方式时,完成与移动终端之间的信息传输;在休闲方式时,SIM 卡将保留所有相关数据,并支持内部全休眠、指令休眠和时钟休眠 3 种休眠方式。

2. SIM 卡与 GSM 基站数据传送、个人化和安全机制

1) SIM 卡与 GSM 基站之间传送的相关信息

在 GSM 基站设置鉴别中心(AUC),为 GSM 网络提供鉴别用户、加密数据和信号所需的全部信息。

在 SIM 卡中,符合 GSM 协议规范,并与用户相关的信息有国际移动用户识别码(IMSI)、密钥 Ki,以及加密算法 A3、A5、A8。

为了避免 IMSI 在传送时被窃取,所以将其转换成临时移动用户识别码 TMSI,同理将 Ki 转换成 Kc,转换方法将在下面说明。A3、A5、A8 算法尚未标准化,仅规定调用算法时的输入/输出信息,但 GSM 系统中已有使用实例,生产手机的各公司都采用它的算法,因此可实现手机漫游。A3、A5、A8 算法固化在 SIM 卡的 COS(片内操作系统)中。

2) SIM 卡的个人化

合法的 SIM 卡必须经过严格的管理步骤才能得以实现。SIM 卡在制造厂家出厂时即应写入该卡的序列号、操作系统码、特定的数据及保密密钥,以便进行个人化处理。一旦这些信息装入后,就不能更改。

在 SIM 卡的预个人化阶段,先将芯片的 E^2PROM 格式化,建立目录结构,开辟 GSM 应用数据文件,以便由网络经营部门将 GSM 业务相关的数据写入这些特定的文件中。在预个人化阶段存储的信息如下:国际移动用户识别码(International Mobile Subscriber Identity,IMSI)、鉴权密钥 Ki、个人识别码(PIN 码)、PIN 码出错计数、预个人化数据、SIM 卡状态、个人解锁密钥 PUK(解锁一般由运营商进行)。其中,IMSI 是全球唯一的识别码。

在 SIM 卡的个人化阶段，将一些特定的信息，如用户相关信息、个人化数据和用户访问等级控制写入 SIM 卡。在预个人化阶段和个人化阶段，写入何种数据是由网络经营者确定的。SIM 卡在进行个人化处理后，数据文件的访问是由 SIM 卡软件控制的，这种控制与规定的保密规则相符。

在手机的控制下可读出或更新加密密钥 Kc、临时移动用户识别码 TMSI、区域识别码和附加 GSM 业务相关信息。另外，还具有短消息业务存储、费率信息存储、缩位拨号、固定号码呼叫、禁止呼出等功能。

3）安全机制

GSM 网络和 SIM 卡间传送的信息都要进行加密，同时加入随机数 RAND，因此即使是同一信息，加密的结果也不相同。如果第 3 方对某些信息或密钥破译，对以后的操作还是无用。

SIM 卡主要用 A3、A5、A8 加密算法，凡是个人化时写入 SIM 卡的信息，在 GSM 网络中也存在，因此用到这些信息时不需要传送。

(1) 鉴权。GSM 网络中的鉴权中心 AUC 鉴别手机的合法性，鉴别过程如下。

SIM 卡将网络生成并传送来的随机数 RAND(128 位)和 Ki 作为输入数据，使用 A3 算法，得到的输出结果称为 SRES(32 位)，传送给手机。手机将计算结果、集成电路标识符、ICCID 返回网络。SIM 卡上的 ICCID 共有 20 位，表示卡的运营商代号，发行的省(市)、供应商、用户识别码及第 20 位的校验码。在鉴权中心 AUC 也将 RAND 和 Ki 使用 A3 算法，得到 SREC，并与 SIM 传来的 SRES 进行比较，如果相等，则鉴权通过，移动电话合法。

(2) 密钥 Kc。对 RAND 和 Ki 施以 A8 算法，计算得到 Kc(64 位)，作为对信息进行加密/解密的密钥。

(3) 信息加密。对网络和 SIM 卡间传送的信息(如命令和数据)，施以 A5 算法后再传送。

上面讲到的 SRES、Kc 和 RAND 称为鉴权三参数，可使用多次(如 5 次)，即不是每次通话都要鉴权。电话号码随卡不随机，通话费用计入持卡用户的账单上。

TMSI 是在 GSM 系统中，对 IMSI 进行 A5 算法加密运算而得(密钥为 Kc)，之后使用的是 TMSI 而不是 IMSI。

2G 手机还有安全隐患，如鉴权是单方的，即不存在 SIM 卡对 GSM 系统的鉴别。

3. SIM 卡的数据结构

(1) SIM 卡数据文件。SIM 卡是按数据文件来组织数据的。同一数据文件的信息具有相同的安全保密特性和数据管理特性。数据文件有两种类型：一种是透明的文件，由固定长度的字块构成；另一种是面向记录的数据文件，它由固定长度的逻辑记录组成。

(2) SIM 卡的目录。在 SIM 卡中，按树状结构组织文件，它有一个根目录(即 MF)，根目录下面有 GSM 应用目录和电信应用目录两个子目录(DF)，另外还有两个数据文件(EF)。根目录内存放着两个应用目录的属性(标识符、类型和起始地址等信息)。两个数据文件是持卡者信息和 IC 卡识别号。GSM 应用目录存储着所辖的各个数据文件的属性(标识符、类型、安全保密特性、长度及起始地址)，这些数据文件存储 GSM 网络操作所需

的信息。

7.3　智能卡的硬件和芯片

7.3.1　智能卡芯片的逻辑结构

从信息技术的角度来看，智能卡的核心技术就包含在嵌入卡内的芯片上，它由三部分组成：微处理器、存储器和输入/输出接口。

对非接触式IC卡来说，还有天线，一般为环绕卡四周的几匝铜线。IC卡通过触点或天线与读写器交换信息，非接触式IC卡的接口部件中还包含射频收发电路和调制解调器。目前所有电路都集成在一个芯片中，是一个片上系统(System on Chip，SoC)。

工作时，除了IC卡刚加电时进行初始化处理外，均以读写器与卡之间的命令-响应对方式工作。微处理器接收从读写器发送来的命令，对之进行分析后，根据需要控制对存储器的访问。访问时，微处理器向存储器提供要访问的数据单元地址(当写时还有数据)，然后由存储器根据地址返回对应的数据给微处理器，由微处理器再对这些数据做进一步处理(读时)；或者将数据写入存储器(写时)。此外，智能卡所需要的运算(如加密运算)也是由微处理器来完成的。在上述这些过程中，如何控制及实现这些过程则是由智能卡的硬件和操作系统来完成的。图7.8所示为智能卡硬件结构框图，天线安置在卡内的四周，触点安置在卡的封面上。

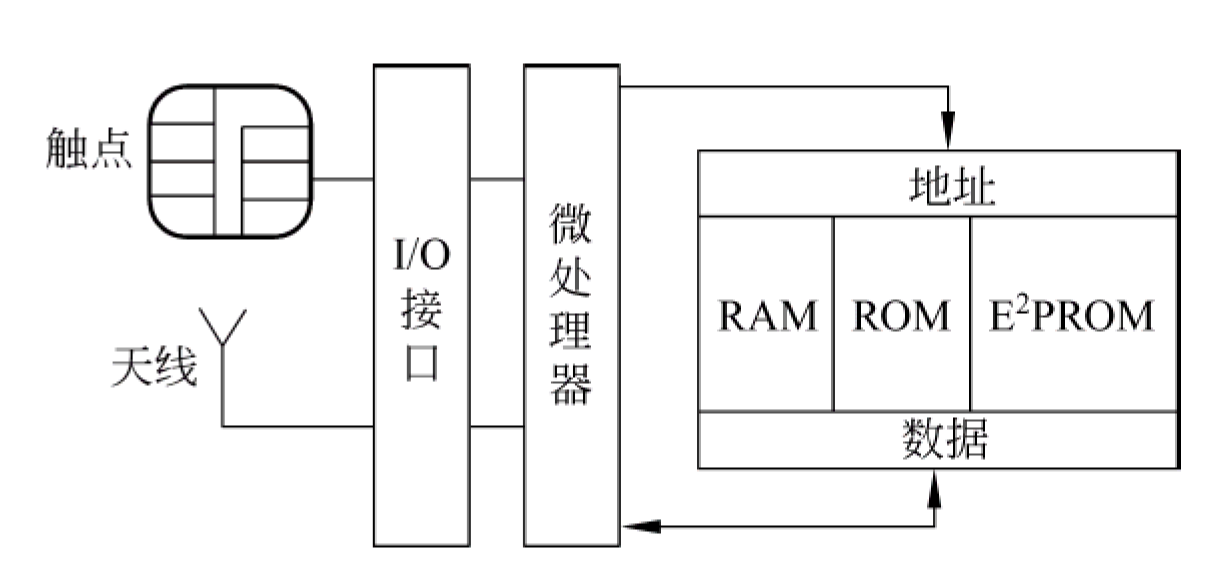


图7.8　智能卡的硬件结构框图

卡内的微处理器又称微控制器(MCU)，它不是专门为卡设计的，而是使用了在计算机控制领域内经过长期考验的工作可靠的微控制器，曾采用Motorola公司的6805系列微处理器(8位)、Intel公司的8051系列微处理器(8位)和ARM公司的ARM微处理器。其中，ARM为32位RISC(精简指令系统计算机)结构的微处理器，当前以ARM微处理器为主。采用8位字长的微处理器主要是由于受到了智能卡芯片尺寸的限制，使得微处理器的内部电路不能过于复杂；而另一个原因也是因为某些智能卡本身所需要的管理工作及所要实现的功能还都比较简单，使用8位微处理器就能够达到要求。为了节省芯片面积，可以将原来在微处理器的某些功能而在IC卡中无用的部分予以删除，如微控制器原来有多个I/O通道与外界联系，而在IC卡中只有一个I/O触点，因此可予以简化。

智能卡通常采用DES、RSA等密码算法以提高安全度。当采用RSA算法时，由于要进行大指数模运算，对微处理器的运算速度要求较高，因此在芯片内一般设置有专用的算

术运算部件。

7.3.2 ARM 微处理器

1. 发展与应用

ARM 微处理器是英国 ARM 公司开发的 32 位 RISC 微处理器，占 32 位 RISC 市场的 75％以上，广泛应用于手机、视频/音频处理、图像处理、机顶盒、数码相机、网络设备和工业控制等许多领域。ARM 公司不直接设计和生产 ARM 芯片，而是以 IP 核（见片上系统）的形式转让设计许可，已授权几十家设计和（或）生产芯片的公司，根据实际应用的需要生产各具特色的芯片，这些公司使用 ARM 核，再加上外围电路，形成自己的 ARM 处理器芯片进入市场。ARM 系列具有功能和性能不同的多种产品，除了执行 32 位 ARM 指令外，还可支持多个指令子集，其中有 16 位指令集 THUMB。该子集有 36 条指令，从部分 32 位指令压缩而来，其目的是减少程序占用的存储器容量，在执行程序时又将 16 位指令实时恢复成 32 位指令。ARM 指令和 THUMB 指令不能混合编程，当处理器处于 ARM 状态时不能执行 THUMB 指令，处于 THUMB 状态时不能执行 ARM 指令。每个指令集中包含有切换处理器状态的指令。加电时首先处于 ARM 状态。

目前已推出 64 位 ARM 处理器。ARM 微处理器具有低功耗、低成本的特点，ARM 不断加快推陈出新的速度，从而加快了授权客户新产品的研究与发行。2014 年推出的 ARM Cortex-A17 主要用于移动和电子消费市场（智能手机和平板电脑），一般高级智能手机已兼有平板电脑的多媒体处理功能。高通公司取得 ARM 最高级指令集的授权，其产品骁龙（Xiaolong）处理器中配备有 4 核 ARM、DSP、GPU（图形显示器）、调制解调器等，是畅销的 SoC。在手机领域、三星、德州仪器公司和中国的华为、中兴都购得 ARM 架构的授权。

其他还有 Intel 公司的 Xcale 和安全性较高的 Strong Secrvre Core 系列 ARM 处理器等。

ARM 已推出 ARM-720GPU（图形处理器）、ARM Mail-V500 Video（视频处理器）、ARM DP500 Display（显示处理器）等产品，相辅相成，解决了多媒体方案的推广应用。

英国 ARM 公司已被日本公司收购。

2. 指令系统

集成电路工艺的发展和应用的推广，促使 ARM 的处理器性能不断提高，下面对采用 RISC 技术的 ARM 微处理器的基本指令系统进行简单介绍，让读者体会一下 RISC 的指令系统与智能卡的命令系统的差异，从而考虑如何通过卡内的操作系统实现智能卡的功能。

1）指令特点

（1）指令格式一致化，从而简化了微处理器的设计与制造。而且在程序运行时，相邻指令可以按流水线方式工作，从而提高了运算速度。

基本指令格式：

操作码	数据地址 1	数据地址 2

（2）寄存器数量多。一般指令的操作都在寄存器之间进行，唯有加载/存储指令（即

读/写指令)访问存储器,访问寄存器比读写存储器快很多。ARM 寄存器数量有 37 个($R_0 \sim R_{36}$),其中 30 个为通用寄存器,必备的是 $R_0 \sim R_{15}$,R_{15}为程序计数器 PC。数据长度为 32 位、64 位。

(3) 程序状态寄存器 PSR。在一般计算机中称为 PSW(程序状态字),共有 6 个程序状态寄存器。其中一个是当前 PSR(CPSR),5 个是保存 PSR(SPSR),当执行中断程序等情况时,当前的 CPSR 内容将改变,在改变前将 CPSR 中的内容保存到一个 SPSR 中。

CPSR 的内容有条件标志码 N、Z、C、V(共 4 位),禁止中断位(2 位),当前执行的指令是 ARM 或 Thumb(1 位)及处理器的其他状态(5 位)。

2) 指令

(1) 访问存储器指令。

① LDR/STR。

LDR:将存储器的数据送寄存器,数据可以是字节、半字和 32 位。

STR:将寄存器的数据送存储器。

② LDM/STM。批量连续存储的数据从存储器的一个区域传送到另一个领域。

③ SWP。寄存器与存储区之间交换数据。

(2) 数据处理指令。

① 数据传送指令。将立即数送寄存器,或者在寄存器之间传送数据。

② 算术逻辑运算。

- 算术运算:ADD/SUB(加法/减法)
  ADC(带进位的加法)/SUC(带借位的减法)
  根据运算结果将 N、Z、C、V 置入 CPSR 的状态位。若结果为负,则 $N=1$;若结果为零,则 $Z=1$;若相加有进位或相减有借位,则 $C=1$;若结果溢出,即超出数据能表示的范围,则 $V=1$。
- 移位指令:寄存器数据进行移位,有算术移位、逻辑移位、循环移位。
- 逻辑运算:AND(与)、OR(或)、EOR(异或),逻辑非。
- 位清除:将寄存器中某几位清零。
- 比较指令:比较两数大小,将运算结果状态置入 CPSR。与 SUB 指令的差别是运算结果不保存。
- 乘法指令有以下几种:32 位×32 位(乘法结果保留 32 位或 64 位);32×32+32(乘加运算);64 位×64 位(乘法,结果 64 位);64 位×64 位+64 位(乘加运算)。

(3) 转移指令。

- 转移指令:无条件转移或根据 N、Z、C、V 状态决定是否转移。若要转移,则将转移地址送到 PC(R15)。
- 调用指令:转移到子程序的指令。除了完成转移指令的功能外,还将当前指令的下一条指令地址送寄存器 R14,即子程序完成后返回源程序的指令地址。

(4) 协处理器指令。

ARM 与协处理器配合工作而向协处理器发出的指令,主要完成 ARM 与协处理器之间的数据传送。

• CDP：协处理器数据操作指令。ARM 通过 CDP 指令的参数向协处理器传递应完成的功能。然后由协处理器自主执行。
• LDC：协处理器数据读取指令。将 ARM 存储器内容(批量)传送到协处理器的寄存器中。
• STC：协处理器数据写入指令。将协处理器的寄存器内容(批量)传送到 ARM 的存储器中。
• MTC：将 ARM 寄存器内容(批量)传送到协处理器的寄存器中。
• MRC：将协处理寄存器内容(批量)传送到 ARM 的寄存器中。

(5) 其他指令。

• SW1：软中断，从用户模式(用户程序)转换到管理模式(操作系统)
• MRS 或 MSR：读或写状态寄存器 CPSR、SPSR(与通用寄存器进行写或读操作)。
• ARM：伪指令。没有定义在 ARM 指令集内，在编译时，将它用等效的 ARM 指令替代之。
• NOP：空操作。可用伪指令处理，如用 MOV R_0，R_0 替代。

7.3.3 SoC 和存储器

1. 片上系统(SoC)

上面讲到的 SoC 是指用标准化的电子功能模块(即已有的微处理器模块)和新设计的功能模块在单一的集成电路芯片上制作的完整系统。这种标准化的功能模块称为知识产权核(如 ARM 核)或 IP 核(Intellectual Property core)，它不是为当前制作的芯片专门设计的，具有可在许多种芯片中快速、可靠和可重复使用的特点。SoC 可以包含多个原来在印制电路板上安装的器件。如今在一个芯片上已经可以集成微处理器、数字信号处理器、逻辑电路、存储器和输入/输出接口等，甚至可将数字电路、模拟电路和射频电路集成在一个芯片中。与全部独立设计的芯片相比，可以缩短开发时间，降低成本，减少错误，快速推向市场。SoC 的胜出得益于微电子工艺的进步而导致的芯片集成度的提高，以及 ASIC(专用集成电路)设计技术的成熟。

DSP(Digital Signal Processor，数字信号处理器)基本上可分为两类，一类是专门为实现某种数字信号算法而设计的专用处理器，一般将其算法固化在芯片的 ROM 中。另一类是通用 DSP，通过编码实现多种数字信号处理算法。

2. 智能卡的存储器

与微处理器一样，智能卡内的存储器由于受到卡的外形尺寸限制，容量一般都不是很大。智能卡的存储器通常由 ROM、RAM 和 E^2PROM 组成。其中，RAM 通常不超过 256B，仅提供给 COS 存储操作过程中的数据；COS 的代码部分(程序)则存储于 ROM 中；E^2PROM 是智能卡的用户真正能够访问的存储区，这一部分存储了智能卡的各种信息、密码及应用文件等，还可能包含 COS 的某些部分。采用 E^2PROM 使得智能卡能够有效地读写数据和停电时保存数据。

由于存储器的容量不大，因此 COS 通常使用直接寻址方式，也就是直接使用物理地址访问存储单元。这样做的好处是可以使读写控制相对简单化，适应了智能卡简便的

要求。

7.4 智能卡的操作系统

随着 IC 卡从简单的逻辑加密卡发展到内带微处理器的智能卡，人们开发了应用于智能卡内部的各种各样的操作系统，也就是在本节将要论述的 COS。COS 的出现大大地改善了智能卡与读写器的交互界面，使智能卡的管理变得更容易、使用更安全，为智能卡的发展开拓了极为广阔的前景。

7.4.1 COS 概述

COS(Chip Operating System，片内操作系统)是紧紧围绕着它所服务的智能卡的特点而开发的。由于不可避免地受到了智能卡内微处理器芯片的性能及存储器容量的影响，COS 在很大程度上不同于通常所能见到的微机上的操作系统(如 Windows 和 Linux 等)。首先，COS 是一个专用系统而不是通用系统。不同卡内的 COS 一般是不相同的。因为 COS 一般都是根据某种智能卡的特点及其应用范围而特定设计开发的，尽管它们完成的功能大部分都遵循着同一个国际标准。其次，与微机操作系统相比，COS 在本质上更加接近于监控程序，而不是真正意义上的操作系统，这一点至少在目前看来仍是如此。因为在当前阶段，COS 所需要解决的主要还是对外部的命令如何进行处理、响应的问题和安全问题。

COS 一般都是紧密结合智能卡内存储器分区的情况，按照国际标准(ISO/IEC 7816 系列标准)中所规定的一些功能进行设计、开发的。但是，由于目前智能卡应用的发展速度很快，而国际标准的制定不能及时跟上，又存在专利和竞争等因素，因而在当前的智能卡国际标准不可能十分完善的情况下，厂家对自己开发的 COS 做了一些命令扩充。就目前而言，还没有任何一家公司的 COS 产品能形成一种工业标准。

COS 的主要功能是控制智能卡和外界的信息交换，管理智能卡内的存储器，并在卡内部完成各种命令的处理。其中，与外界进行信息交换和确保安全是 COS 最基本的要求。

读写器与 IC 卡之间的通信，是全部通过 COS 进行的，对某些数据，如密码和密钥，是绝对不允许从卡内传送到卡外的。当 IC 卡发给持卡人后，COS 的程序代码(即使是部分代码)也是绝对不允许泄露到卡外的。存放在 ROM 中的 COS 代码，甚至对卡的发行人也是保密的。如果有下载到 E^2PROM 中的部分 COS 代码，相对于 ROM 来说比较容易泄密，需要特别注意遭受攻击的可能性，要防止攻击者下载另外一些程序到 E^2PROM 中，以致改变了原 COS 程序的一些功能，从而造成巨大损失。

由于卡内微处理器的指令比 IC 卡的命令简单得多，因此每条命令的功能都通过 COS 中的一段程序实现。

7.4.2 一个简单的 IC 卡操作系统(SCOS)示例

为了引导读者对智能卡 COS 内部结构的理解，本节设计了一个非常简单的操作系

统，命名为 Simple COS(SCOS)。该卡设想应用于单位内部的小额消费(一卡专用)，基于非常小的存储器容量，但符合 ISO/IEC 7816 国际标准。

该卡的存储器由 ROM、RAM 和 E^2PROM 组成，复位应答信号 ATR 与 COS 存放在 ROM 中；文件和数据存放在 E^2PROM 中；安全状态和 I/O 缓冲器(如存放当前执行的命令 APDU 和响应 APDU 的缓冲器)等的即时信息放在 RAM 中，在 IC 卡加电时，有必要对 RAM 中一部分内容进行初始化，设置成默认值。

1. SCOS 的文件系统

SCOS 的文件系统结构如下。

(1) SCOS 有两层文件 MF 和 EF，由于是一卡专用，而且功能比较简单，因此不再设置 DF 文件。

(2) SCOS 的内部基本文件(EF)有 3 个：存密码的 SF、存密钥的 KF 和存系统信息的 AF。内部基本文件仅供 COS 访问，采用透明结构。

(3) SCOS 的工作基本文件(EF)有 3 个：一个存放余额的 PF、一个存放交易记录的 RF 和一个保存个人信息的 IF。其中，PF 和 IF 采用透明结构，RF 采用定长记录的环形结构。

(4) SCOS 用唯一标识符(2 字节)访问文件，定义如下。

MF：3F00；SF：2F01；KF：2F02；AF：2F00。

PF：4F00；RF：4F02；IF：4F03。

(5) EF 文件由文件头和文件体两部分组成，SCOS 采用文件头和文件体分开相向存放法，即将文件头集中在一起，并从 E^2PROM 最小地址(0000)开始存放；文件体也放在一起，并从 E^2PROM 最大地址开始存放。这样的安排便于增添新文件。若将 E^2PROM 的 0000～02FF 空间(共 768B)用于存储文件，则可画出图 7.9 所示的 SCOS 文件系统在 E^2PROM 中的存储空间分配。在图中没有专设 MF 文件体存储空间，而将所有的文件头(从 AF 到 IF)都视为 MF 的文件体。文件头中包括的内容有文件标识符、该文件体在 E^2PROM 中的起始地址、文件体的长度和访问(读/写)条件等。为简化设计，假设每个文件头的长度是相同的。

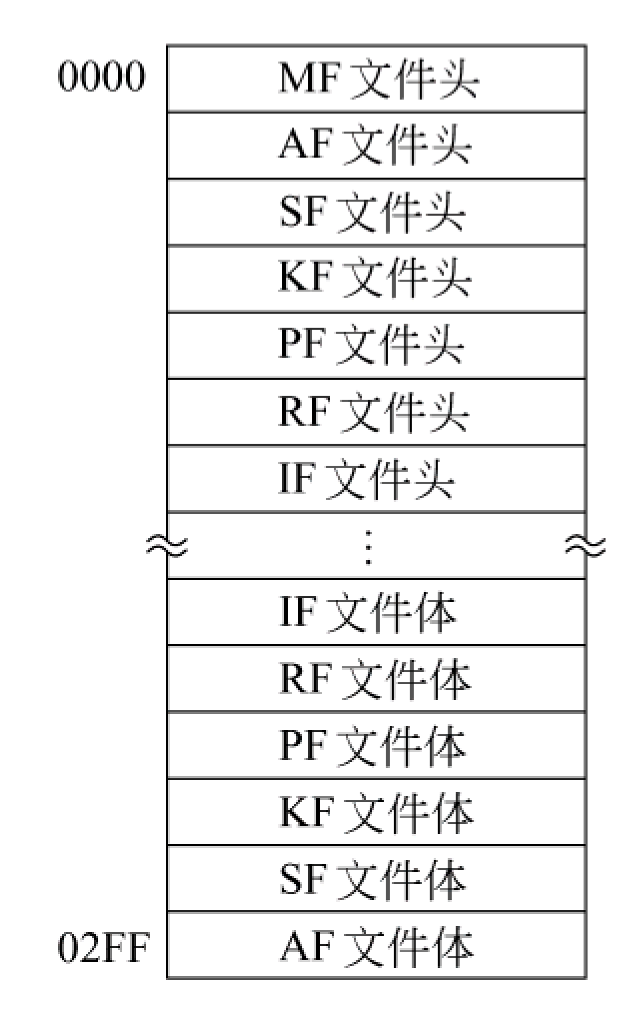


图 7.9 E^2PROM 文件存储区分配

2. 安全管理和应用管理

有关安全部分需要考虑 3 个问题：安全状态的建立、安全属性的设置及安全机制的实现。SCOS 采用以下方案。

使用两个密码：发行商密码 ISC 和持卡人 PIN。当 IC 卡插入读写器时，只有当从键盘上输入的密码与卡内先前存入的 ISC 或 PIN 相同时，才能核实插卡人的身份是发行商还是持卡人，或者都不是，然后才允许进行读/写操作。因此，需要将核实的结果保存下来，用来控制其后某些操作的执行权限，直到卡拔出为止。一旦卡拔出，核实结果不再有用。下次插卡时，要重新核实插卡人的身份。SCOS 在 RAM 区内选定一个单元(长度设为 1B，b_0～b_7)

存放安全状态字，定义如下。

- b_0：外部鉴别位(卡判别读写器真伪)，卡执行外部鉴别命令，如果读写器为真，则将 b_0 置 1。
- b_1：PIN 核实位，如果核对个人(使用人)密码正确，将 b_1 置 1。
- b_2：ISC 核实位，如果核对发行商密码正确，将 b_2 置 1。
- $b_3 \sim b_7$：保留于将来使用。

当卡插入读写器，复位后应立即将安全状态字清除为全 0，只有在相应的验证通过后才能分别将 b_0、b_1 或 b_2 置 1。于是就可用安全状态字进行安全管理和应用管理了。表 7.1 列出了安全状态字与允许卡进行的操作之间的关系。

表 7.1　安全状态字与允许卡执行的操作

安全状态字			卡允许执行的操作
b_2	b_1	b_0	
×	×	0	允许执行外部鉴别命令，如果通过，将 b_0 置 1
0	0	1	允许验证 ISC 或 PIN，核实后，将 b_2 或 b_1 置 1
×	1	1	已核实 PIN，允许持卡人消费或修改 PIN，填写交易记录
1	×	1	已核实 ISC，允许增加卡内余额(持卡人存钱)

为了实现表 7.1 的功能，在每个文件的文件头中设置了该文件的“读/写”条件(1 字节)，称为安全属性。对保存余额的 PF 文件，设置了如下 8 位条件码。

b_3	b_2	b_1	b_0	b_3	b_2	b_1	b_0
×	×	1	1	×	1	×	1
读条件				写条件			

其中，读条件用来控制查询余额或消费，写条件控制增加余额(充值)，各位的意义与安全状态字中的 $b_3 \sim b_0$ 对应。在对文件进行操作时，把 RAM 中的安全状态字和 E^2PROM 文件头中的安全属性比较，仅当匹配(即相符)时才允许进行操作。另外，在对文件进行操作前，读写器与卡之间要进行相互(双向)鉴别，除了 IC 卡要对读写器进行外部鉴别外，还需要读写器对卡进行内部鉴别，以确定读写器和卡的真伪，后者的鉴别结果可以不保存在卡中。如果读写器发现卡是假的，将中止操作。

保存交易记录(日志)的 RF 文件采用环形结构，其记录数可根据需要确定，如果设计定为 10 条，则可保存最近进行的 10 次交易记录。也就是说，在记满 10 条记录后，如有新的交易产生，将替换掉最早保存在卡中的记录。新记录总是被定为 1 号记录，在此之前刚写入的记录为 2 号记录。

除了在文件头中规定了安全属性外，在命令系统中也可为每条命令设置各自的安全属性，仅当安全条件与命令中的安全属性相符时才允许执行该命令。

在卡发行时或发行前，发行人可根据实际需要设计文件结构、文件数量和文件的安全属性。但当卡发给持卡人后，一般就不允许再修改了，这也是为了安全。

3. 传送管理

传送管理用来处理 SCOS 与读写器之间的信息交换，遵循 ISO/IEC 7816-3 国际标准

的规定，有 $T=0$ 和 $T=1$ 两种协议，SCOS 选择较为简单的 $T=0$ 协议。卡加电后向读写器发送 ATR，然后双方以命令-响应对的方式进行通信。在卡的 RAM 存储区开辟一块区域作为信息缓冲器，用来暂存命令 APDU、响应 APDU 和外部输入的信息（如 PIN 和消费金额等），以实现读写器与卡之间的通信。

4. 命令系统

当 IC 卡接收到一个命令 APDU 后，首先对命令的合法性及安全条件进行检查，通过后再根据该命令所要完成的功能进行操作，最后将执行的结果（响应 APDU）返回给读写器。以上这些工作都是由预先设计好并存在于 ROM 中的操作系统（COS）控制卡内微处理器完成的。

SCOS 中设计的命令如下。

(1) 文件处理命令。创建文件、选择文件和删除文件。

(2) 安全管理命令。取口令（取随机数）、内部鉴别、外部鉴别和验证密码（PIN 和 ISC）。

(3) 应用命令。读二进制、写二进制、读记录和写记录。

其中，创建文件命令只能在卡发行之前执行。

5. 防意外掉电

在智能卡工作时，防止因突然掉电或用户随意插拔智能卡而造成写入数据出错。一般智能卡中没有在掉电时仍维持一段时间电压的功能，因此一旦掉电，卡中的软件立即无法执行。在本例中，如果在修改卡中余额时产生这种情况，其后果是严重的。前面已经讲到，文件是建在 E^2PROM 中的，而 E^2PROM 进行写入（或修改）操作有两个步骤：首先是擦除，然后才写入。如果正好在擦除与写入之间掉电，卡中的余额将不再是正确的了。因此，对 COS 提出一个要求，对卡中的某些功能要么完整地实现，要么完全不进行。将不可分割的完全满足这一要求的进程称为“原子进程”。为解决此问题，在 E^2PROM 中设置了一个缓冲区，用以接收数据，在其中还包含一个状态标记，用来表示该缓冲区内容“有效”或“无效”。

工作过程如下：首先将被修改的原始数据及其地址复制到缓冲区，并将状态标记设置成“缓冲区内容有效”；然后把新数据写入到原来该写入的地址，如果能完成这一操作（不发生掉电），则将状态标志设置成“缓冲区内容无效”，否则（掉电）仍保持为“缓冲区内容有效”，并中止进一步的操作。当智能卡再次上电时，SCOS 被启动，在它发送 ATR 以及读写器和 IC 卡的双向鉴别后，查询“缓冲区状态标记”，如果是“有效”的，则将缓冲区的数据按所存地址写入 E^2PROM，从而恢复了原始数据，消除了上一次上电后所进行的“不完整”操作的影响。这种机制能保证文件中的数据（无论是否意外掉电）有效。

上面叙述的方法有两个缺点。第一个是在所有的 E^2PROM 中，上述缓冲区将具有最频繁的擦除/写入负担，由于 E^2PROM 中任何给定区域的擦除/写入次数是有限的，因此这个缓冲区可能就是 E^2PROM 中首先开始发生写错误的部分，而使智能卡不能再使用。解决的办法是增加缓冲区容量，采用循环结构，分段使用缓冲区以分散负担。第二个缺点是在写访问时对缓冲区的强制性访问增加了 SCOS 的执行时间。

6. SCOS 在一次消费交易中完成的操作

图 7.10 所示为正常情况下的操作流程，当任一环节出现异常时，将中止操作。图中每一方框是卡接收读写器发出的命令后，在卡内 SCOS 控制下，由卡内微处理器执行一段

程序(称为子程序)完成指定的功能。另外需要注意的是,在对某一文件进行访问时,该文件必须为当前文件,而且,只能有一个文件为当前文件,因此在图7.10中,多次执行选择文件命令。

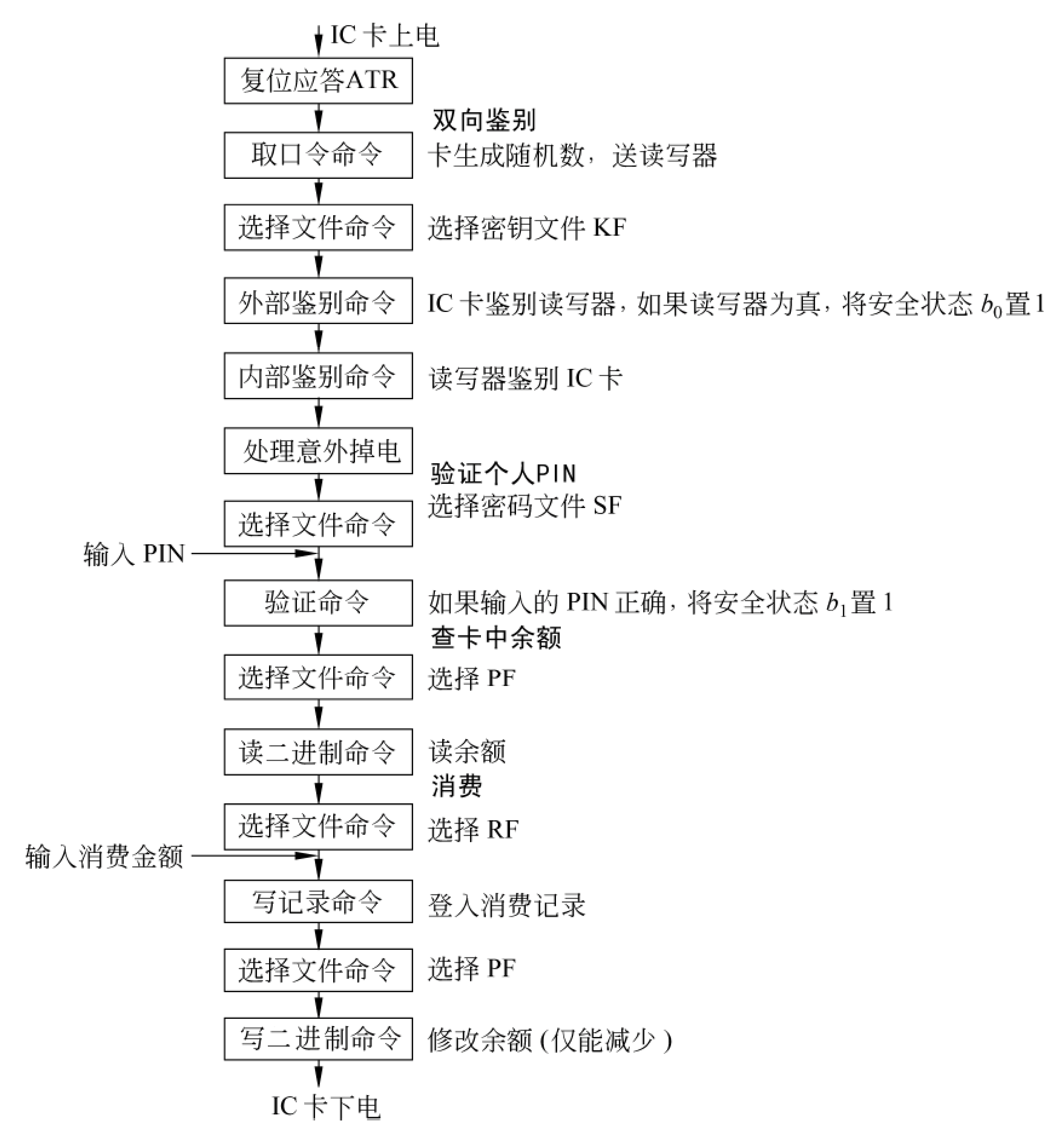


图 7.10　SCOS 在一次消费交易中完成的操作流程

以上叙述的是持卡消费的过程,如果需要在卡内追加金额,可去指定地点充值,其操作流程大致与消费过程相同,但以下两点必须执行。

(1) 将输入 PIN 改为输入发行商密码 ISC,比较相符时将安全状态 b_2 位置 1。

(2) 将消费金额改为存入金额,并加到 PF 文件的余额中。

7.4.3　COS 的体系结构

COS至少解决3个问题,即文件操作、鉴别与验证、安全机制。事实上,鉴别与验证和安全机制都属于智能卡的安全体系的范畴之中,所以,智能卡的COS中最重要的两方面就是文件与安全。但再具体分析,实际上可以把从读写器发出命令到卡给出响应的一个完整过程划分为3个部分,也可以说是3个功能模块:传送管理器、安全管理器、应用和文件管理器,如图7.11所示。其中,传送管理器用于检查信息是否被正确地传送,这一部分主要和智能卡所采用的通信协议有关;安全管理器主要是对所传送的信息进行安全

性的检查或处理，防止非法的窃听或侵入；应用和文件管理器则用于判断所接收的命令执行的可能性，通过验证命令的操作权限，最终完成对命令的处理。对于一个具体的COS命令而言，这3个部分并不一定都是必须具备的，有些可以省略，或者是并入另一部分中。以下将按照这3个部分对COS进行较为详细的论述。

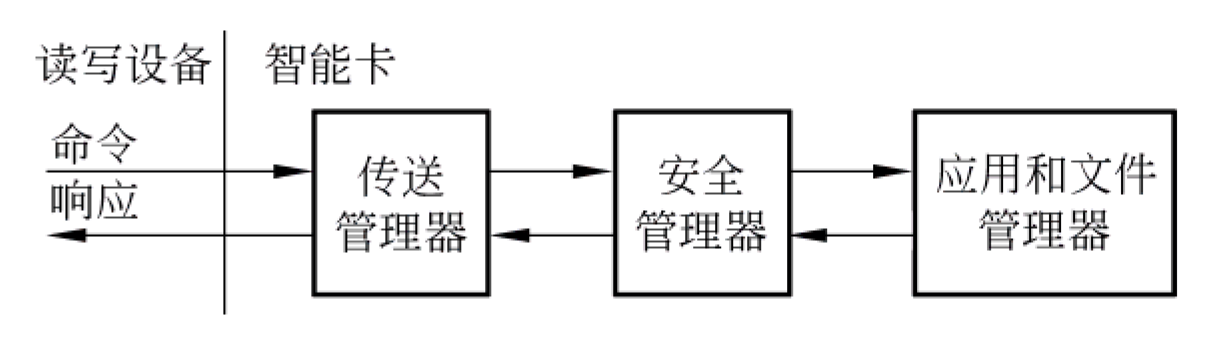


图7.11　命令处理的过程

1. 传送管理器

传送管理器(transmission manager)主要是依据智能卡所使用的信息传输协议，接收读写器发出的命令，处理后，把对命令的响应按照传输协议的格式发送出去。由此可见，这一部分主要和智能卡具体使用的通信协议有关。而且，所采用的通信协议越复杂，这一部分实现起来也就越复杂。

传送管理器在对命令进行接收的同时，也要对命令接收的正确性作出判断。这种判断只是针对在传输过程中可能产生的错误而言的，并不涉及命令的具体内容，因此通常是利用诸如奇偶校验位、校验和等手段来实现。当发现命令接收有错后，不同的信息交换协议可能会有不同的处理方法：有的协议是立刻向读写器报告，并且请求重发；有的则只是简单地做一标记，本身不进行处理，留待它后面的功能模块做出反应。这些都是由协议本身所规定的。

第6章中指出：每条命令的CLA字节指示该命令的命令-响应对是否按安全报文SM传送，若是，而且命令APDU和响应APDU的数据都存在，则将命令APDU的Lc、数据、Le字段加密成密文，并加入密码校验和字段，响应APDU增加密码校验和。如果不按安全报文传送，则加入一般的校验和，主要作用是检查传输是否有错。

如果传送管理器认为对命令的接收是正确的，那么，它将接收到的命令的信息部分传到下一功能模块，即安全管理器，而滤掉诸如起始位、停止位之类的附加信息。相应地，当传送管理器在向读写设备发送响应时，则应该对每个传送单位加上信息交换协议中所规定的各种必要的附加信息。

2. 安全管理器

智能卡的安全体系(security structure)是智能卡的COS中一个极为重要的部分，它涉及卡的鉴别与验证方式的选择，包括COS在对卡中文件进行访问时的权限控制机制，还关系到卡中信息的保密机制。可以认为，智能卡之所以能够迅速地发展并且流行起来，其中的一个重要原因就在于它能够通过COS的安全体系给用户提供一个较高的安全性保证。

安全体系在概念上包括三部分：安全状态(security status)、安全属性(security attributes)及安全机制(security mechanisms)。其中，安全状态是指智能卡在当前所处的一种状态，或称为安全环境(security environment)，这种状态是在智能卡进行复位应答或在它处理完某命令之后得到的。安全状态通常可以利用智能卡在当前已经满足的条件的

集合来表示。安全属性实际上是定义了执行某个命令或访问某个文件所需要的一些条件,只有智能卡满足了这些条件,该命令才是可以执行的。因此,如果将智能卡当前所处的安全状态与某个操作的安全属性相比较,那么根据比较的结果就可以很容易地判断出一个命令或文件在当前状态下是否允许执行或访问,从而达到了安全控制的目的。和安全状态与安全属性相联系的是安全机制。安全机制可以认为是增强安全状态所采用的方法和手段,通常包括通行字验证、密码鉴别、数据鉴别及数据加密/解密等。把增强了的安全状态与某个安全属性相比较,如果一致,就表明能够执行该属性对应的命令,这就是COS安全体系的基本工作原理。

从上面对COS安全体系的工作原理的叙述中可以看到,相对于安全属性和安全状态而言,安全机制的实现是安全体系中极为重要的一个方面。没有安全机制,COS就无法进行操作。而从上面对安全机制的介绍中可以看到,COS的安全机制所实现的就是如下功能:命令的判断、鉴别与验证、数据加密与解密、文件访问的安全控制。因此,将在下面对它们进行介绍。

(1) 鉴别与验证。鉴别与验证其实是两个不同的概念,但是,由于它们二者在所实现的功能上十分相似,因此同时对它们进行讨论,这样也有利于在比较中掌握这两个概念。

通常鉴别(authentication)指的是对智能卡(或读写器)的合法性的鉴别,即是如何判定一张智能卡(或读写器)不是伪造的卡(或读写器)的问题;而验证(verify)是指对智能卡的持有者的合法性的验证,也就是如何判定一个持卡人是经过了合法授权的问题。由此可见,二者实质都是对合法性的一种认证,就其所完成的功能而言是十分类似的。但是,在具体的实现方式上,由于二者所要认证的对象不同,所采用的手段也就不尽相同了。

具体而言,在实现原理上,验证是通过由用户向智能卡出示只有他本人才知道的通行字PIN或生物标志,并由智能卡对它的正确性进行判断来达到验证的目的。在通行字PIN的传送过程中,有时为了保证不被人窃听,还可以对要传送的PIN进行加密/解密运算。

(2) 密钥管理。COS把数据加密时要用到的密钥组织在一起,以文件的形式储存起来,称为密钥文件。最简单的密钥文件就是长度为8个字节的记录的集合,其中的每个记录对应着一个密钥;较为复杂的密钥文件的记录中则可能还包含着该记录所对应的密钥的各种属性和为了保证每个记录的完整性而附加的校验和信息,其结构如图7.12所示。其中的记录头部分存储的就是密钥的属性信息,如是可以应用于所有应用文件的密钥还是只对应某一应用文件可用的密钥。但是,不论是什么样的密钥文件,作为一个文件本身,COS都是通过对文件访问的安全控制机制来保证密钥文件的安全性的。

记录头	密钥(64位)	校验和

图7.12　密钥文件的记录结构

当需要进行数据加密运算时,COS就从密钥文件中选取密钥加入运算。从密钥文件中读出密钥时。为了避免多次使用同一密钥,从而给窃听者提供破译的机会,安全性不太高。因此,可对密钥本身做一些处理,尽量减少其重复出现的机会。例如,对从密钥文件中选出的密钥首先进行一次DES加密运算,然后将运算结果作为数据加密的密钥使用。

其计算式为

$$Key = DES(CTC, K_s)$$

式中，K_s 是从密钥文件中选取的一个密钥；CTC 是一个记录智能卡的交易次数的计数器，该计数器每完成一次交易就增 1；Key 是最后要提供给数据加密运算使用的密钥，每次交易采用的 Key 都不相同。使用这种方法可以提高智能卡的安全性，但却降低了执行效率。上例中的 CTC 可以用其他值（如随机数）替代。

3. 应用和文件管理器

应用管理器主要解决智能卡中的应用实现问题。智能卡的各个应用都与文件和命令有关。文件是指关于卡内数据单元和（或）记录的有组织的集合。COS 通过给每种应用建立一个对应文件的方法来实现它对各个应用的存储及管理。因此，COS 的应用文件中存储的都是与应用有关的各种数据或记录。

COS 的文件按照其所处的逻辑层次可以分为 3 类：主文件 MF、专用文件 DF 及基本文件 EF。可以用树状结构来形象地描述一个 COS 的文件系统的基本结构。

7.4.4 SCOS 程序举例

前面讲述了 COS 的体系结构，而在智能卡具体进行处理时，除了卡激活时返回复位应答 ATR 外，其后所采用的都是命令-响应对的方式。

下面以编写图 7.10 中的“复位应答 ATR”和“读二进制命令”子程序为例，启发编写 COS 的思路。先画出子程序操作流程图，并指出完成子程序所需的微处理器指令。存储器 RAM、ROM 和 E^2PROM 是统一编址的。

1. 微处理器程序流程示意图

微处理器程序流程如图 7.13 所示。

2. 实现程序流程的存储器

存储器如图 7.14 所示。

3. 实现程序流程所需的微处理器指令

① 转移指令：转子程序指令（或称为调用指令）和返回指令（返回到上层调用程序）；条件转移指令。

② 读写指令：访问存储器。

③ 算术运算指令：加法指令、减法指令。

④ 比较指令。

上述程序的编写，与微处理器的指令系统和程序设计人员的习惯相关。

图 7.13 中用到的指令都可以在 ARM 的指令系统中找到。

4. 逻辑通道

在智能卡中，各条命令的 CLA 字段都指出执行本条指令的逻辑通道。逻辑通道的含义如下。

在执行 SELECT（选择）命令时，将命令 APDU 的 CLA 所指定的逻辑通道作为当前的逻辑通道，并选择一个文件（DF 或 EF）为当前文件，后续程序应在当前的逻辑通道和当前的文件中执行。如果在后续程序中，命令的 CLA 指定的逻辑通道号与当前的逻辑

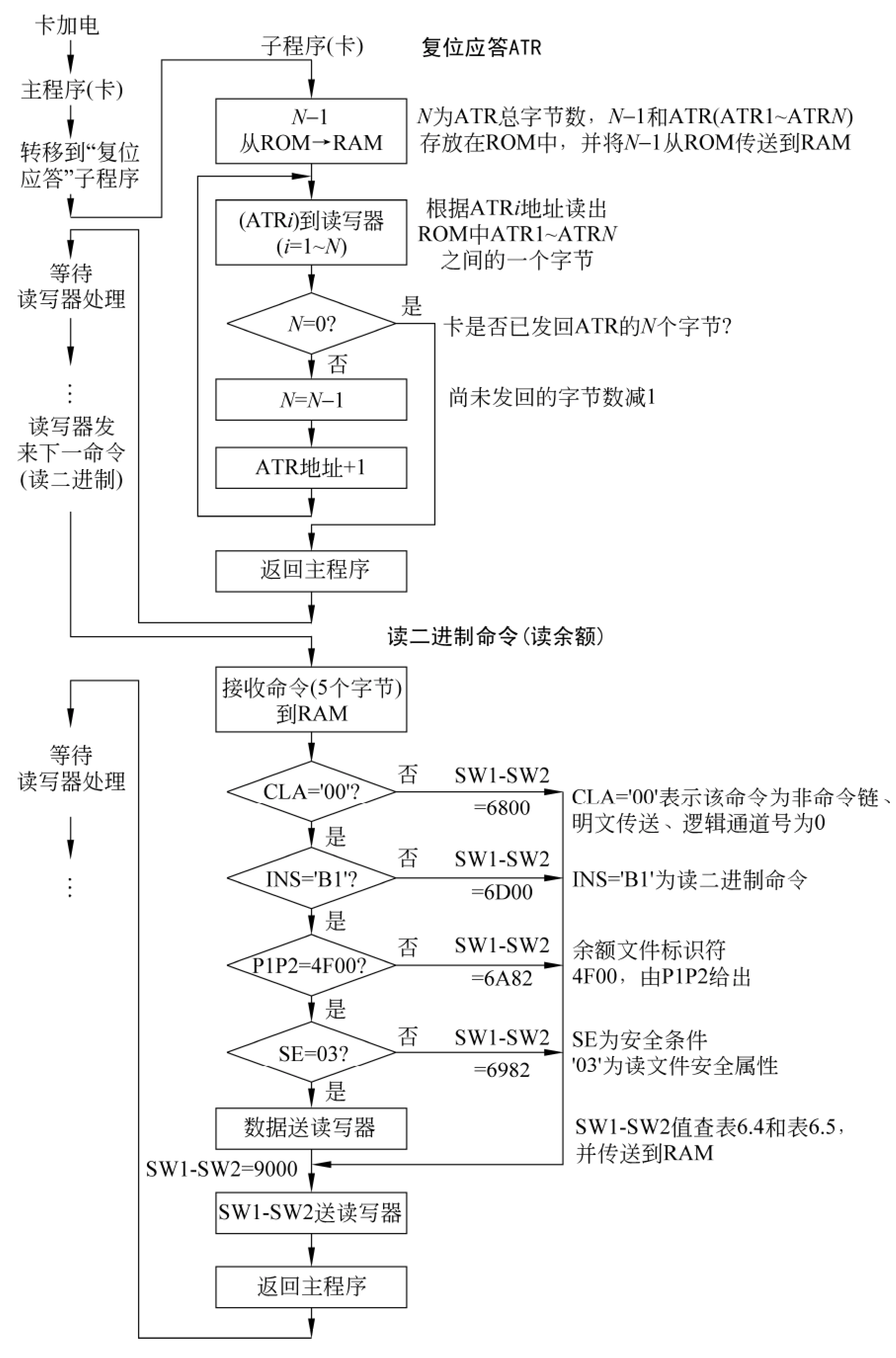


图 7.13 微处理器程序流程示意图

通道号不同,则停止本条命令的执行,并进行相应的处理;如果程序设计者有多道程序设计的观念,则可在多个通道上执行程序,从宏观上可理解为并行执行多道程序,由于在硬件只有一个物理通道,因此在卡中称它为逻辑通道。

在 SCOS 中,仅使用一个编码为 0 的逻辑通道。

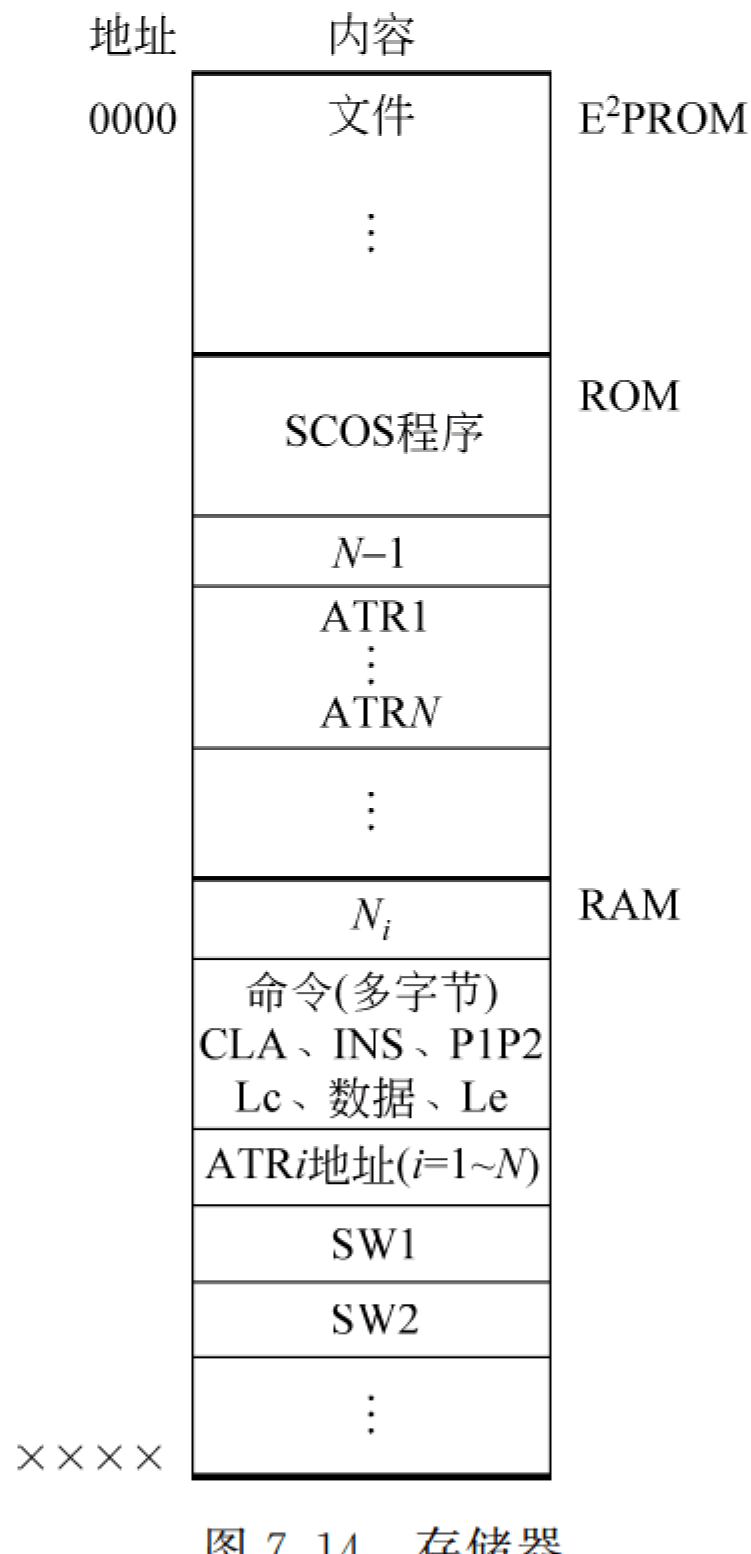


图 7.14　存储器

7.5　COS 设计原则与测试

7.5.1　COS 设计原则

智能卡与外界(读写器)之间的联系必须通过 COS 才能进行，在程序执行过程中卡的安全和数据存取时的保护极为重要。由于受到卡内可用存储器数量的限制，COS 只能占有少量存储空间，一般在 3～20KB。

1. COS 的编程语言

COS 一般用汇编语言编写，这样可使编译后的程序代码占用较少的存储空间。如果用 C 语言编写，即使经过高度优化，也比用汇编语言编写的具有同样功能的程序代码多占存储器 20%～40%的空间，同时其运行速度也较低。然而，其最大的问题还在于它所需的 RAM 量，RAM 的存储密度要比 ROM 和 E^2PROM 低很多，因此从限制芯片尺寸考虑，RAM 存储器的资源在卡中是极其有限的。用汇编语言编程也有缺点，它通常比 C 语言编程更容易产生错误。采用独立的完全可测试的模块化设计，有利于及时发现编程错误。COS 程序编写好后，一般存入 ROM 中，当芯片生产出来以后，ROM 中的程序代码无法修改，如果有错误，将导致整批芯片报废，影响效益和声誉，因此不能忽视测试和质量保证工作。

设计者一旦选定微处理器后，有关生产厂家(公司)可提供 COS 的开发工具，但这要

在双方通过协商并签订合同后才能实现，保证安全是首先要考虑的问题。

2. 程序代码结构

ROM 中的内容是在生产芯片时写入的，写入后就不能修改。根据应用对卡的安全性、成本和修改错误难易程度的不同要求，COS 的程序代码在 ROM 和 E^2PROM 存储器中有不同的分配方法，叙述如下。

(1) 把尽可能多的程序代码放在 ROM 中，因此，所有 COS 程序的核心部分及其余的重要部分都存储在 ROM 中，只允许一小部分程序存储在 E^2PROM 中。

(2) COS 的程序代码全部在 ROM 中，只把数据存储在 E^2PROM 中。

设计者根据安全要求、生产成本、芯片面积及可靠性等，综合考虑后选定代码结构。

3. 存储器的构成

在卡中有 3 种不同类型的存储器。ROM 只能在芯片制造期间通过掩膜来编程，而且是一次编完永不改变。RAM 在电源加到卡时才能保持内容，掉电就会丢失数据，卡加电时需要初始化，如将安全状态字清 0。RAM 可以进行无限次写入，且操作速度快；E^2PROM 可以在没有外加电源情况下保持数据，但有 3 个缺点，即有限的擦/写次数、较长的擦/写时间(约比 RAM 长一万倍)和按区(或按行)擦除的结构。另外，IC 卡在每次加电后最好能对存储器进行测试，如果发现错误，一开始就排除掉或中止操作。

4. 智能卡文件

所有文件都可通过两个字节的代码(文件标识符)寻址。当智能卡个人化时(即准备发给持卡人时)，所有文件都被创建并装入智能卡内。

文件内容分成两部分：文件头和文件体。文件头内包含文件的格式和结构，以及存取条件等信息；文件体存储数据。

文件的成功选择将导致之前选择的文件无效，即在任何时候被选中的文件只能有一个，该文件称为当前文件。

文件访问条件(安全属性)编码在文件头中，文件管理的安全性立足于对文件访问权限的管理。在文件创建时就规定了访问条件，以后不能再改变。

在 EF 文件中，附加有文件属性的定义，这些属性取决于卡的应用领域，设置的目的是防止对 E^2PROM 操作可能产生的写差错。这些属性在文件创建时被规定，在以后一般是不可改变的。有以下几种文件属性。

(1) WORM 属性。一次写，多次读。把一串代码一次性永久写入一个文件中。例如，在卡个人化时，将持卡人的姓名和卡使用截止时间永久性写入卡中，写入后不能再修改。该属性可以用硬件或软件实现。

(2) 多重存储属性。由于 E^2PROM 的擦除/写入次数是有限制的，对某些文件的频繁写入有可能使有关的 E^2PROM 位失效。通过在写入数据时存储其多重备份，读出数据采取多数表决的方法来清除失效位的影响，对写数据，通常采用 3 重并行写入存储，对读数据采用了 3 中取 2 的多数表决方式。

(3) 差错检测码(EDC)利用属性。利用 EDC 可检测到错误。与其他方法一起采用，有可能纠正错误。

(4) 原子操作属性(见 7.4.2 节的“防意外掉电”)。在写入操作时，要么完整地执行，

要么根本不执行。由于这种机制要花费两倍多的写操作时间，因此只能有选择地在需要的文件中进行。

在前面介绍的文件头（文件描述符）中至少包含以下条目。

① 文件名，如 FID='2000'。

② 文件类型，如 EF。

③ 文件结构，如线性记录（定长、变长）、透明记录。

④ 文件长度，如 10 条记录。

⑤ 存取条件，如读/写在 PIN 验证之后。

⑥ 属性，如 WORM。

⑦ 链接到父文件，如链接在 MF 之下。

最后需要强调的是，编写完的 COS 要进行严格的测试。

7.5.2 COS 的测试

1. 测试原则

(1) 测试要求详尽、全面，对卡应完成的全部功能都要进行测试。当输入不正确的命令或操作有误时，测试程序(COS)应自动中止，给出发生差错的信息，并且不能改变卡中原来存储的有关数据，以便于查出错误的原因。

(2) 在硬件设计和 COS 设计阶段就要考虑测试方案，为此在芯片中可能会附加一些测试专用电路，设置一些观察点和熔丝等，在完成测试或个人化后将熔丝断开，从而限制以后某些操作的执行，以维护卡的安全。在设计 COS 时也应考虑如何划分程序模块，以便于调试与测试。

(3) IC 卡从设计、生产到最后的产品出来，要经历多个步骤，每一步都可能产生废品，为了及早将不合格的中间产品检测出来，原则上每经过一道工序都要进行检测。

(4) COS 和硬件存在的问题会交叉在一起，要认真检查。

2. 设计工具与测试仪器

在完成了硬件设计以后，就可进行 COS 设计，在设计 COS 的过程中，不排除对硬件实行局部修改的可能性。接触式 IC 卡的硬件包括 MCU、存储器(RAM、ROM 和 E^2PROM)和与触点连接的接口电路，将其集成在一个芯片中。

COS 的设计一般在半导体生产厂家提供的工具上进行，该工具包括两部分：仿真 IC 卡（用于测试读写器）和仿真读写器（用于测试 IC 卡）。

(1) 仿真 IC 卡。具有被设计的 IC 卡的所有功能部件，但由集成度较低的若干个现成的芯片和一些附加电路构成。其中，ROM 由 RAM、EPROM 或 E^2PROM 替代，以便将设计中的 COS 写入仿真卡存储器后，可修改 COS 的内容，在设计过程中这种情况是经常发生的。另外，仿真 IC 卡最好能有自诊断能力，这样在调试 COS 程序时，在某些场合可很快区分是硬件还是软件问题。一般自诊断在加电后立即进行。

仿真 IC 卡（接触式）通过 6 个或 8 个触点与外界接触。

仿真 IC 卡（非接触式）通过天线与外界接触。

(2) 仿真读写器。功能是产生调试 COS 程序所需提供给各触点的信号，并接收与分

析从 IC 卡返回的信息。

在向 IC 卡加电时，提供各触点激活 IC 卡所需的时序信号；在下电时，提供 IC 卡停止工作各触点所需的时序信号，接收并分析从 IC 卡返回的复位应答。

发送测试程序（命令 APDU 组成）和接收响应 APDU，并分析。非接触式 IC 卡中的 COS 增加防冲突程序。

3. 测试举例（SCOS 的测试）

下面以 SCOS 为例来说明有关测试的问题。测试的方法与步骤是可以改变的，原则上以正确、全面为准，而且与卡处于生命周期哪一阶段有关，还与测试目的有关。例如，检测成品卡是否合格和寻找问题卡出错原因、出错地点，其检测程序一般是不同的。

1）SCOS 设计阶段

（1）模块化设计。一般的大程序在完成软件的总体设计以后，将其分成若干个功能独立的模块（程序），并明确各模块之间的输入/输出要求，这样就可以有多人同时参加模块程序的编写，各模块分别调试后再进行模块之间的联调。SCOS 的程序很简单，不一定需要多人共同完成程序的编写，但考虑到模块功能明确，调试方便，并且还能减少程序量，节省存储器空间，所以仍考虑采用模块化设计。可分为以下模块。

① IC 卡加电、断电处理模块。内容包括如下部分。

- 加电后，对 IC 卡硬件的初始化（设置默认值）。
- 防插拔（防意外）。如果上次交易影响写入的正确性，在此纠正；为防止本次交易突然停电而进行的预处理（防意外掉电）。
- 发送 ATR 到读写器。

② 命令-响应对的公共处理模块。

- 命令 APDU 中 CLA 和 INS 编码合法性处理。
- 响应 APDU 中的 SW1、SW2 编码设定。
- 安全条件和安全属性匹配性检查（包括加密/解密算法的实现）。

③ 各命令 APDU 的专有处理模块。

- 各命令参数（P1、P2）和数据字段（Lc、data、Le）编码合法性处理。
- 命令功能的实现。

（2）编程语言。采用 IC 卡中的 MCU 所支持的汇编语言编写 SCOS 程序，在微机上将其编译成 MCU 的二进制机器语言（指令）代码，并存放在仿真器的 RAM 或 EPROM 中（由仿真器决定），其优、缺点分别如下所述。

RAM 修改方便、速度快，但仿真器掉电会丢失内容，而这是经常会发生的，所以需要有后备存储保留备份，在加电时将其内容复制到 RAM 中。EPROM 掉电时仍能保持内容，但修改内容比较麻烦，需用紫外线先擦除其内容随后才能写入。因此，也可以考虑用闪存或 E^2PROM 暂存设计过程中的程序。

另外，还希望能实现反汇编，即将存储器中存放的 SCOS 二进制程序代码转换成用 MCU 指令表示的汇编程序，以便于人工检查 SCOS 的正确性。

（3）编写测试程序并进行程序模块调试。在仿真读写器中编写测试上述各模块的测试程序，并将相应信号转换到各触点上。

如果 SCOS 中编写的程序还与频率有关，则需要进行变频测试。

如果在模块测试过程中发现问题，要及时修改 SCOS 程序，修改后要重新进行测试。在测试时，除了检查在正常工作情况下的操作结果是否正确以外，还要尽可能检查所有在不正常情况下的操作结果是否与预期的相同，一定要保持卡内数据的安全。

在完成了程序模块的分调和联调后，就可考虑运行更为复杂的测试程序，具体内容可参考下面介绍的 IC 卡操作系统测试程序举例。

测试通过后，提交厂家生产，在芯片生产过程中将 SCOS 写入 ROM。

2）试制芯片的测试

试制芯片除了要测试 SCOS 外，还要考验硬件的正确性和可靠性，并且要注意某些命令(如创建文件)在个人化后就不能再执行了，因此要在个人化前进行充分的测试。

3）成品测试

批量生产的芯片要全部(100％)进行测试，封装卡后还要再进行 100％测试。

4）IC 卡操作系统 SCOS 测试程序举例

主要考虑 IC 卡的测试，但可供设计阶段和生产阶段的测试作参考。

测试程序可以多样化，此例仅作参考。

建议测试步骤如下。

(1) IC 卡加电，返回 ATR，与正确的 ATR 比较，如果相同，进入下一步；否则，中止执行测试程序。

以下不设置安全属性，对能正常执行的文件处理命令和应用命令进行测试。

(2) 任意建立一个二进制文件，选择该文件，再执行写二进制命令和读二进制命令。

每执行一条命令后，检查卡的响应 APDU 是否与预期的一致。

(3) 建立 SCOS 中定义的其余 5 个文件。

(4) 轮流选择各个文件，进行写入(写二进制/写记录)与读出，并检查是否会影响非当前被选文件的内容。

(5) 删除文件，被删文件不应再被选择。

以下对安全管理命令进行测试。

(6) 执行取口令命令，获取随机数，然后执行外部鉴别命令。应成功执行，并设置相应的安全条件码(是否能设置，要靠其他命令来验证)。

(7) 执行内部鉴别命令，如果不成功，中止程序执行。

(8) 建立多个有不同读写条件的文件和密码、密钥文件(SF、KF)。

(9) 执行验证密码(持卡人的 PIN 和发行商的 ISC)命令，应设计有成功执行和不成功执行的多种情况，卡应自动设置相应的安全条件码。

(10) 执行写读文件的命令。并返回第(9)步，重复循环执行。在验证各种安全条件码后进入第(11)步。

步骤(1)～(10)对 IC 卡在正常操作条件下的基本功能进行了测试。每条命令(除步骤(9)和步骤(10))返回的条件码 SW1-SW2 应为 9000，如果测试过程中发现错误，SW1-SW2 不等于 9000，立即中止测试，根据测试程序停止位置，可以判断执行哪条命令时出错。

步骤(11)和步骤(12)对本卡不用的 INS 和 CLA 进行测试。

(11) 当命令的 INS 未被定义时,是否能返回期望的 SW1-SW2。

(12) 测试命令的 CLA 不符合指定值时是否返回预期的 SW1-SW2。可任意选择一条命令,如读二进制文件命令。

以下对每一条命令进行详尽的测试。

(13) 创建文件命令。对命令 APDU 中 P1、P2、Lc、DATA、Le 设置成不同值时,检查响应 APDU 返回的内容,并检查本命令执行后可能出现的所有 SW1-SW2。当出现错误时,不应对卡产生不该有的影响。

(14) 其他命令。所有命令都要一一进行测试。最后根据应用情况进行综合测试。

5) 其他测试

对 IC 卡而言,除了 COS 以外,还要保证硬件的可靠性,所以除了在标准电压和标准频率下进行测试外,还要考虑在电压和频率变化在±5%时 IC 卡工作的可靠性。在变压和变频后重复执行前面介绍的测试程序。

另外,还需要进行防插拔测试。

为了考验卡的可靠性,可以在批量生产的 IC 卡中,随机抽取一些卡片,改变测试的环境温度,循环执行上述测试程序考验一段时间。

6) 卡的个人化处理

由于 SCOS 比较简单,除了个人化后不能再执行创建文件命令以外,其他功能都没有变化,因此大量测试工作可在个人化之前进行。在对少量 IC 卡进行个人化后的详尽测试并证明 SCOS 是正确的以后,大批量的 IC 卡可以在发卡前进行个人化。

7.5.3 智能卡的生命周期

智能卡的生命周期一般可分成 5 个阶段:设计与制造、卡的初始化、个人化、使用和使用终结,如图 7.15 所示。

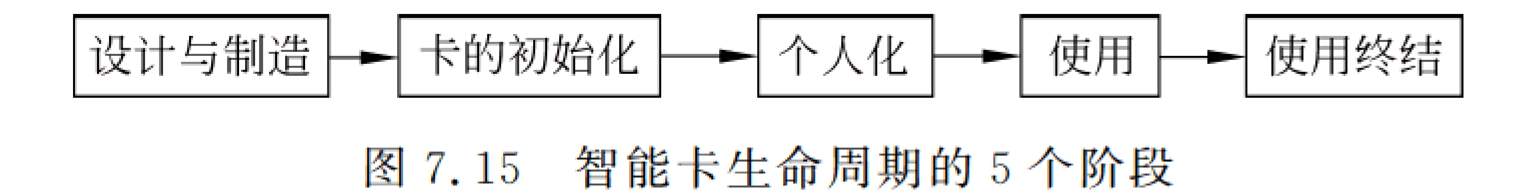


图 7.15 智能卡生命周期的 5 个阶段

智能卡通常应用在以安全为关键的领域中,在生命的第 1 阶段,在设计芯片和操作系统及制造芯片过程中,对安全问题的关注,放在十分重要的地位。如果有秘密数据从卡中读出来,那么该卡就毫无用处了。

1. 智能卡设计与制造

一张智能卡基本上由两个性质不同的部件组成:包含芯片的模块和塑料卡体。智能卡的制造是一个大批量生产过程,如我国的第二代身份证和交通卡等。所有的生产步骤,必须有一定的质量保证和检验(测试)。

根据用户对卡的应用与安全要求设计卡内芯片,确定其功能与指标,并根据工艺水平与成本对卡内处理器的性能和存储器容量等提出具体要求,同时也对片内操作系统提出具体要求。然后就可进行具体设计和制造。

图 7.16 所示为智能卡设计与制造的流程图。在图中，将制好的芯片安装在有 8 个触点微型印制板上，并称为模块。对于非接触式 IC 卡，也要安排好测试点，并为连接天线和测试作准备。

目前卡内集成电路一般包括微处理器(如 ARM)、ROM、RAM、E^2PROM 和安全逻辑等内容。卡内所有电路集成在一个芯片上称为片上系统(SoC)。

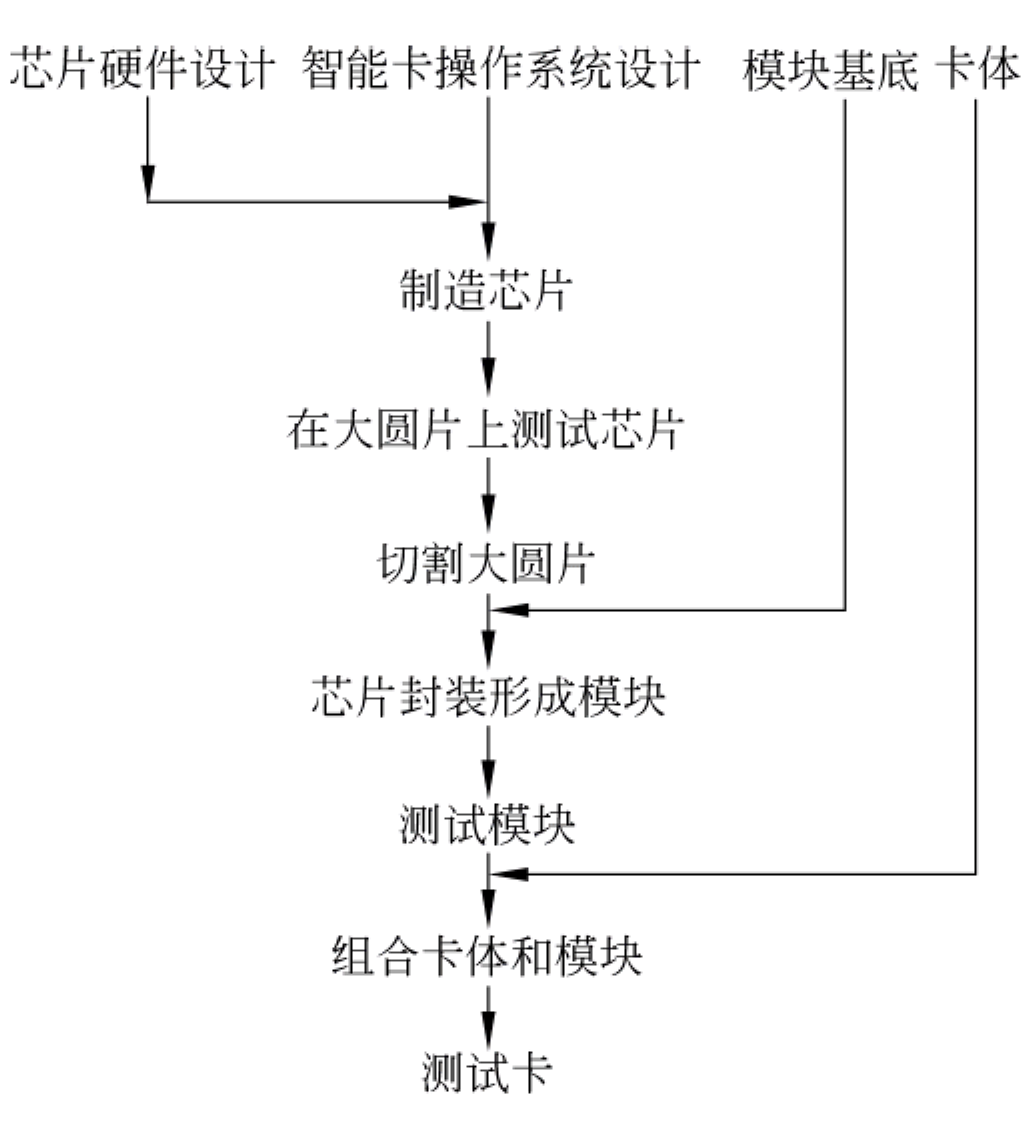


图 7.16　智能卡设计与制造的流程图

2. IC 卡的初始化

将芯片的制造厂标识号、运输码等信息写入 E^2PROM 中，经测试合格后，烧断熔丝，使 IC 卡从测试方式转入用户方式。为安全起见，绝不允许从用户方式再回到测试方式，此时卡可运输给发行商。

制造厂标识号等也可在生产阶段写入 ROM 中。

由于智能卡没有足够的引出端可连到内部电路，为便于测试，可增加一些测试专用的连接线，而烧断熔丝后，这些连接线不再起作用，此后，内部一些保密信息和工作状态不能在外部测到，保证了安全。

3. 个人化和发行

智能卡通过以上步骤制造好以后，制造商通过保密渠道将成批的卡片运输给发行商(银行、邮局和医院等单位)。发行商通过读写器对卡进行个人化处理，使每张卡成为唯一能识别持卡人的卡，发行给最终的客户。

个人化工作大体包括 4 个方面：E^2PROM 分区、写入个人信息、设定个人密码和写入密钥。IC 卡由制造商生产出来后，其应用存储空间(给用户用的而非卡本身使用的空间，通常在 E^2PROM 中)是一片空白，只是在某些特定位置(如制造商的标识号码)有信息。卡到了发行商手里，发行商就要对卡的存储区进行分区，规定这个区派什么用场，那个区有什么用。

发行商还将识别卡的一些信息写入卡内。例如，标识发行商的号码、用户账号、用户姓名和金额等。为保护持卡人而设定的个人密码(或称个人识别号码)也在发行时由用户输入(或由发行商输入，用户拿到卡后可立即修改)，并存储在一个以后连发行商都无法读取的空间内，这通常是由芯片内的安全逻辑予以保证的。

完成了这些过程的卡就成为一张独立的、能唯一标识用户的卡(通过制造商标识，发行商标识，发行号、卡的序列号或账号就可唯一标识一张卡)。经过个人化的卡可由发行者交给用户，用户以后就可凭卡消费或作为证件使用了。

4. 使用阶段

可按各种卡的使用规定进行操作，要求安全、可靠和方便，如果由于设计或制造上的缺陷而造成用户的损失，应由发行方负责。

5. 使用终结阶段

可按标准要求，撤销卡的应用，结束卡的使用，并由发行商收回。而实际上，一般在销毁后就被扔掉了。

最后需要说明的是，由于发行的卡在遵循标准的条件下，可以有不同的用途、设计思想和制作过程，因此在基本符合上述卡的生命周期的叙述情况下会有差异。

习题

1. E^2PROM 的擦除、写入是怎样定义的？它的读出和写入时间与 RAM 相比有什么特殊之处？
2. 在验证逻辑加密卡持卡人身份时，是否允许将 PIN 从卡中读出并送到读写设备中去进行比较？简述其原因。
3. 当用户输入错误的 PIN，且输入次数已达到卡所允许的最大次数时，为安全起见应采取什么措施？该措施需由用户设定还是由卡自动完成？如果金融卡中还保存有余额，应该作废还是应该设法让用户不受损失或少受损失？
4. 智能卡芯片内包含哪些内容？各起什么作用？
5. 如果 IC 卡芯片设计得好，可以保证绝对安全，即可杜绝一切作弊和非法行为。这种说法对吗？
6. 在什么情况下希望在芯片内部设有数字信号处理器(DSP)？主要完成什么功能？
7. CPU 卡中的微处理器一般是新设计的还是采用经过实际使用考验过的设计方案？
8. 什么是 COS？为什么要设计 COS？COS 和一般微处理器的操作系统有什么主要差异？
9. COS 主要存储在卡内什么地方？COS 如何处理内部 EF 文件和工作 EF 文件？
10. 在 COS 中怎样处理意外掉电或任意插拔 IC 卡的情况？如果不处理会产生什么后果？
11. COS 一般由哪几部分组成？各部分的主要功能是什么？在测试 COS 时要注意哪些问题？
12. 简述 COS 在一次交易过程中应完成的基本操作。
13. 设计 COS 时一般用什么编程语言？为什么？
14. 智能卡可以设计得比逻辑加密卡更安全的原因是什么？
15. 在 IC 卡进行设计制造等过程中要进行多次测试的原因是什么？

第 8 章　射频识别技术基础

电子标签(非接触式 IC 卡和 RFID 标签)通过无线射频传送数据方式与读写器联系。本章讲述射频识别基本知识,为后续章节学习无线通信、电子标签和物联网做准备。

8.1　射频识别系统结构

1. 射频识别系统简介

射频识别系统一般由电子标签、读写器和天线三部分组成,RFID 标签与读写器之间的通信是通过空间介质(无线方式)实现的,通信从读写器发送载波信号开始。电子标签可以从天线接收到的载波信号(射频电磁波)中获取能量,经过检波(整流)、倍压、稳压得到工作所需的直流电压。图 8.1 所示为其工作原理,在该图中,通过 A 点与 D 点的是数字信号,通过 B 点与 C 点的是被调制的载波(射频)信号,MCU 为控制部件。

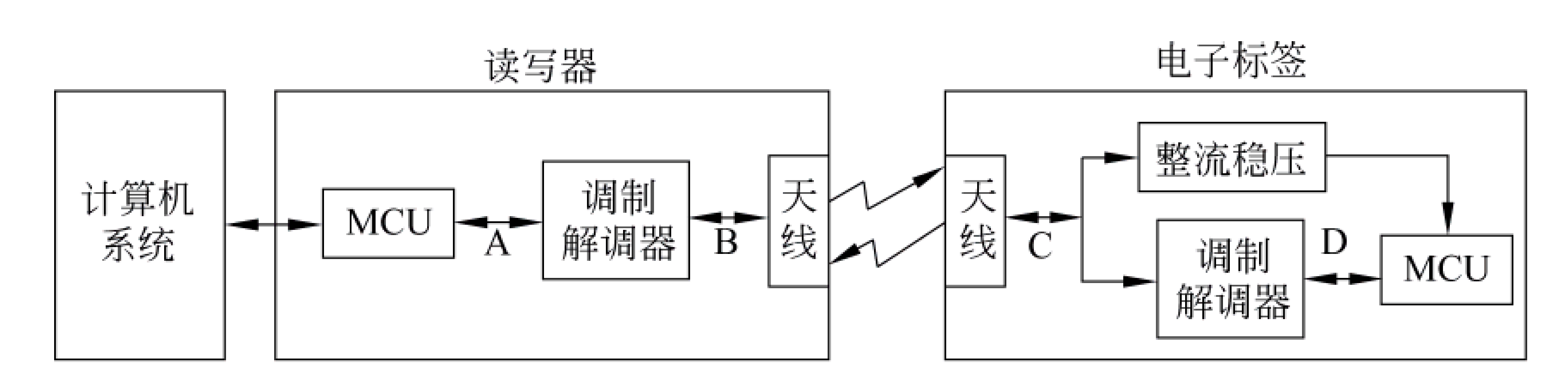


图 8.1　电子标签与读写器通信工作原理框图

2. 电子标签的供电方式

非接触式 IC 卡受卡的厚度限制,卡内不能安置电池,因此是无源 IC 卡。

RFID 标签由芯片和天线构成,根据 RFID 标签内部构造可分为 3 种:有源、无源和半无源标签。带有电池的称为有源(active)标签,不带电池的称为无源(passive)标签。有源式标签使用内部的电池来进行无线通信,因此比无源式标签的通信距离要长,不过会受到电池寿命的限制,它的价格也比无源式标签高,体积也比较大。此外,还有一种内置电池的 RFID 标签,平时不发出电波,当收到读写器的信号时,才发出电波进行通信,标签内的芯片或传感器使用电池来工作,而由读写器负责无线通信,这样的标签称为半无源式标签(semi-passive)。

3. RFID 的频率特点

工作于 13.56MHz 的非接触 IC 卡在我国与世界上已广泛应用,相应的国际标准见第 9 章。

1) RFID 的工作频段

通常情况下,RFID 读写器发送的频率称为 RFID 系统的工作频率或载波频率。RFID 的工作频率不仅决定着 RFID 系统的工作原理、识别距离,还决定着 RFID 标签及

读写器实现的难易程度和设备成本。RFID 技术按照工作频段可分为低频(Low Frequency,LF)、高频(High Frequency,HF)、超高频(Ultra High Frequency,UHF)和微波(Micro Wave,MW)。不同频段下的 RFID 系统具有不同的特点,在读写范围、读写速率和使用环境要求等方面也都不同。

(1) 低频标签。低频标签的典型工作频率为 125kHz 和 133kHz。低频标签一般为无源标签,其工作能量通过电感耦合方式从读写器耦合线圈的辐射近场中获得。阅读距离一般情况下小于 10cm。典型应用有动物识别、容器识别、工具识别和电子钥匙等。

(2) 高频标签。高频标签的典型工作频率为 13.56MHz。该频段标签工作原理与低频标签完全相同,即采用电感耦合方式工作。高频标签的阅读距离一般小于 1m。高频标签的数据传输速率快,已广泛应用于金融卡、居民身份证、电子钥匙、市民卡和门禁卡等。

(3) 超高频标签。超高频标签的典型工作频率有 433.92MHz、860~960MHz。超高频射频标签可分为有源标签与无源标签两类。超高频通过电磁波传递能量和交换信息,阅读距离一般大于 10m,有源标签阅读距离可达百米。超高频射频标签主要用于物流、铁路车辆自动识别、集装箱识别、托盘和货箱标识等。

(4) 微波标签。微波标签的典型工作频率有 2.45GHz 和 5.8GHz。微波标签也分为有源标签和无源标签两类,工作原理与超高频射频标签相同,即通过电磁波的发射和反射来传递能量和交换信息,其阅读距离大于 10m,有源标签阅读距离可达百米。微波射频标签主要用于公路车辆识别与自动收费、托盘和货箱标识等。

2) 双频标签与双频系统

从识别距离和穿透能力的特性来看,不同工作频率的表现存在较大差异。低频具有较强的穿透能力,能够穿透水、金属和动物等导电材料。但在同样功率下,传播的距离较近,又由于频率低,可用的频带窄,数据传输速率较低,并且信噪比低,容易受到干扰。高频相对低频而言具有较远的传播距离、较高的传输速率和较大的信噪比,但其绕射或穿透能力较弱,容易被水等导体介质所吸收。

利用高频和低频的各自长处设计识别距离较远和穿透能力较强的双频产品,可应用于动物识别、导体材料干扰和潮湿的环境。

双频标签有有源标签和无源标签两种。

双频 RFID 系统主要应用于距离要求、多卡识别和高速识别的场合,如供应链管理、人员流动跟踪、动物跟踪与识别、采矿作业和地下路网管理及运动计时等。

4. 天线

天线是电子标签和读写器的空中接口,根据频率识别系统的基本工作原理,两者之间的射频耦合有两种方式:电感耦合方式(变压器型)和反向散射耦合方式(雷达型),在 8.2 节中讨论。

射频接口能将接收到的电磁波转换成电流信号,或者将电流信号转换成电磁波,天线既可以集成到读写器和标签中,也可以设置在外部。

1) 标签的天线

天线应具备以下性能:足够小的体积,可嵌入到本来就很小的标签内;具有全球或半球覆盖的方向性;都应与读写器的信号相匹配;天线能提供足够大的信号给标签内的

芯片。

在选择天线时要考虑以下因素：天线的类型、阻抗、射频性能，以及有其他物品围绕贴标签物品时的射频性能。

标签的使用有两种形式：一种是标签移动，通过固定安置的读写器进行标识；另一种是标签移动或不移动，用手持读写器等进行识别。

2）读写器天线

射频系统的读写器必须通过天线来发射能量，形成电磁场，对射频标签进行识别，并向射频标签提供生成电源的能量。

读写器天线应满足以下条件：天线线圈的电流产生足够大的磁通量；功率匹配，充分利用磁通量；保证载波信号传输的带宽。

在进行应用系统设计时，读写是要考虑的重要指标之一，取决的因素有读写器类型、放置方向、电磁干扰、读写器发射的能量、天线类型，以及读写器或标签所用的电池充电或更换的安排等。

8.2 射频技术

8.2.1 基带信号与载波调制信号

1. 数据一般有数字和模拟两种表达方式

接触式 IC 卡和读写器之间的数据以 0、1 两种状态出现，用高、低电压呈现的方波形式表示（数字信号），其所占据的频带为直流或低频，称为基带信号。而在电子标签中，数字基带信号必须经过高频调制才能进行传输，该高频信号称为载波（模拟信号）。模拟数据的值是连续变化的，如用温度测量的温度和用正弦波表示的信号都是模拟信号。图 8.2 所示为采用调幅方式的信号，有载波输出表示 1，无载波输出表示 0。

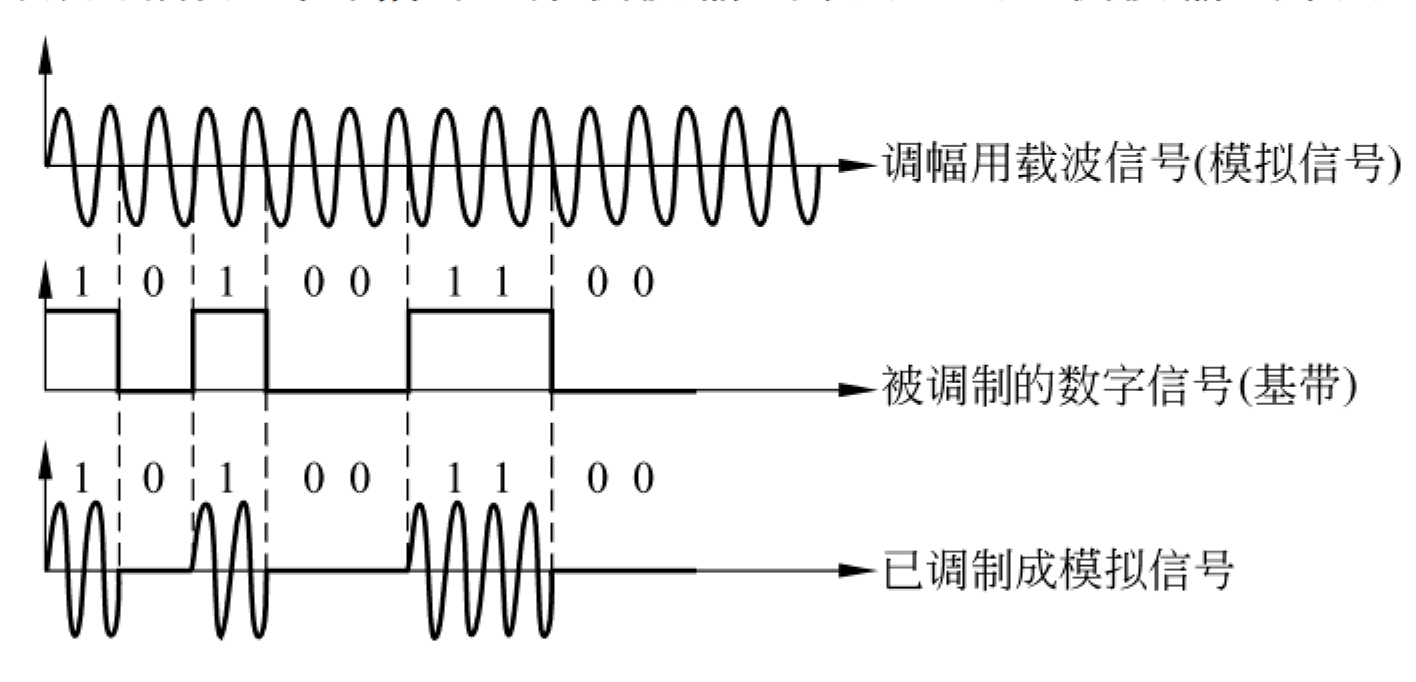


图 8.2　载波调幅信号

在电子标签和读写器的存储器中存放的是基带数字信号，将其转换成高频信号的过程称为调制。在接收端，将高频信号转换成基带数字信号的过程称为解调。实现数据传输的电路称为射频接口。

2. 带宽与宽带

在模拟领域，带宽是指在信道中传输的信号所占的频率宽度，比如能传送的信号频率

范围为 2002～2022MHz。则其带宽为 20MHz，即(2022－2002)MHz 的差。在数字领域，以 0、1 两种状态表示的基带信号，其带宽是指每秒钟能传输的位数，如 12Mbps。

宽带是指当传输率达到一定值时，运营商将“带宽”称为“宽带”(如未达到则称为窄带)，所以“宽带”是满足一定“带宽”值的服务标准。

8.2.2 数字信号的编码方式

常用的基带数字信号的编码有不归零制(Non Return to Zero，NRZ)编码、曼彻斯特(Manchester)编码、双相差异(Differential Bi-Phase，DBP)编码、米勒(Miller)编码、变形米勒(Modified Miller)编码、脉冲间隔编码和脉冲位置编码等方式，如图 8.3 所示。

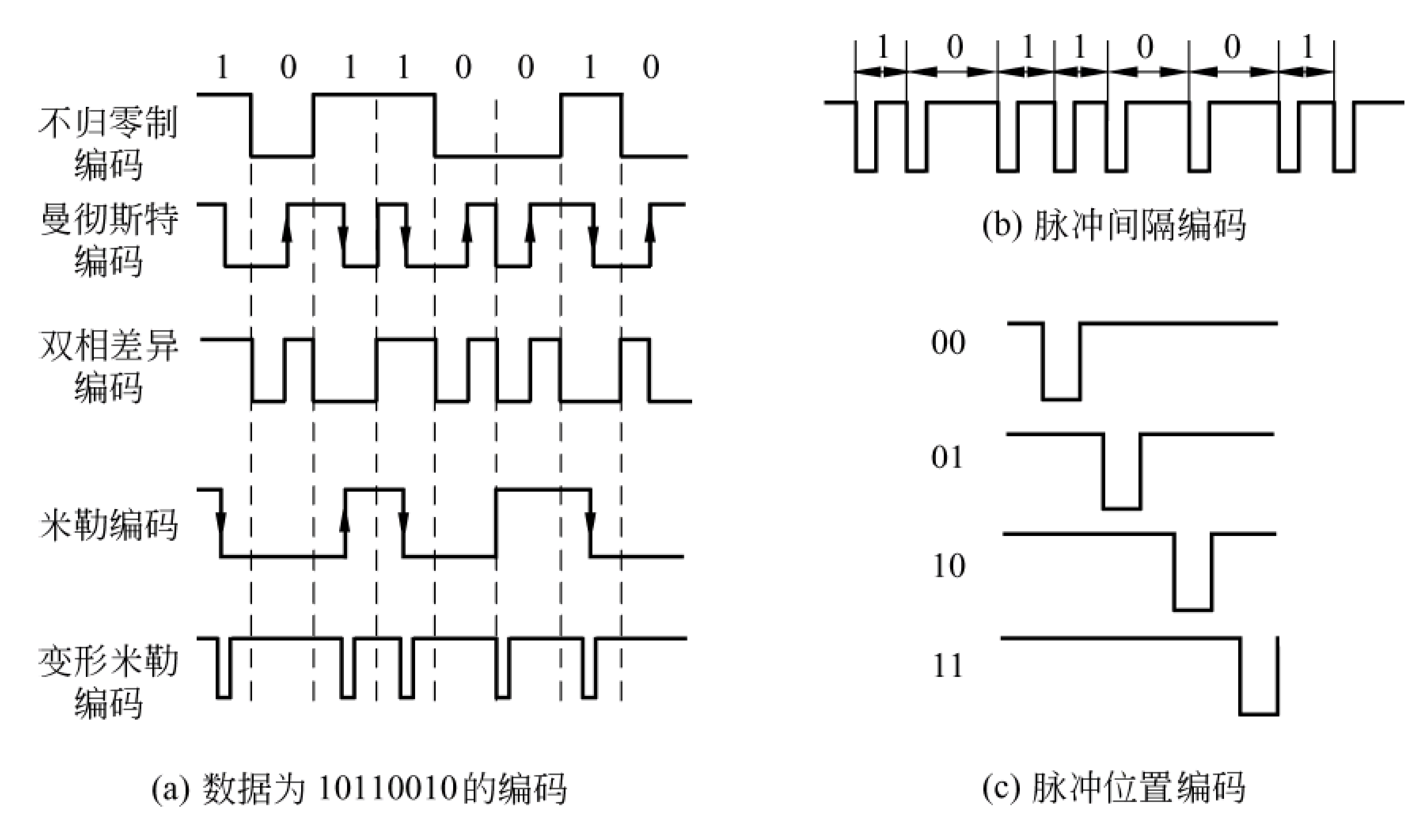


图 8.3 基带数字信号的编码

(1) 不归零制编码。用高电平表示 1，低电平表示 0。

(2) 曼彻斯特编码。在半个位周期的负跳变表示 1，正跳变表示 0，又称为调相编码。在接收端重建同步信号比较容易。重建同步信号是指将接收到的信号，通过设计的电路，可形成同步信号(相当于时钟信号 CLK)。

在图 8.3 中的不归零制编码，当出现连续的 0 或连续的 1 时，信号处于不变的低电位或高电压，因此利用它无法产生同步信号。

(3) 双相差异编码。在半个位周期的正/负跳变表示 0，无跳变表示 1，或相反表示 1 和 0，又称为调频 FM 编码。此外，在每个位周期开始，电平都要反向，在接收端重建位同步比较容易。

(4) 米勒编码。在半个位周期的正/负跳变表示 1，在其随后的位周期内不发生跳变表示 0。而一连串的 0 在位周期开始时发生跳变，又称为改进调频 MFM 编码。在接收端重建位同步也比较容易。

(5) 变形米勒编码。将米勒编码的正/负跳变用负脉冲来代替，就成为变形米勒编码。

(6) 脉冲间隔编码。用两个脉冲间的间隔时间表示二进制数 0 和 1，如用间隔 t 表示

1,2t 表示 0(或反之),如图 8.3(b)所示。因此,0 和 1 的位周期是不同的。

(7) 脉冲位置编码。每个位周期的时间宽度是一致的,在 4 取 1 的编码方式中将 1 个位周期分成 4 段,如图 8.3(c)所示。在第一个时间段出现脉冲表示 00(2 位数),在第二、三、四时间段出现脉冲分别表示 01、10、11。

8.2.3 调制方式

数字信号的调制过程类似于对高频载波信号的开关控制,经常称为数字键控。用基带数字信号控制载波的振幅、频率和相位,分别称为幅移键控(Amplitude Shift Keying, ASK)、频移键控(Freguency Shift Keying,FSK)和相移键控(Phase Shift Keying,PSK),利用高频载波在幅度、频率或相位上的两种状态表示二进制数字 0 和 1。

1. 幅移键控

以载波的幅度大小(或有、无)表示 0 或 1,如图 8.4 所示。当振幅为 u_1 时表示 1,为 u_0 时表示 0(或反之),用以表示 u_1 和 u_0 的变化程度称为调制度或调制系数 m,且 $m=(u_1-u_0)/(u_1+u_0)$。当调制度为 100% 时,又称之为 OOK(On-Off Keying)键控,此时 u_0 的振幅=0,如图 8.4 所示。

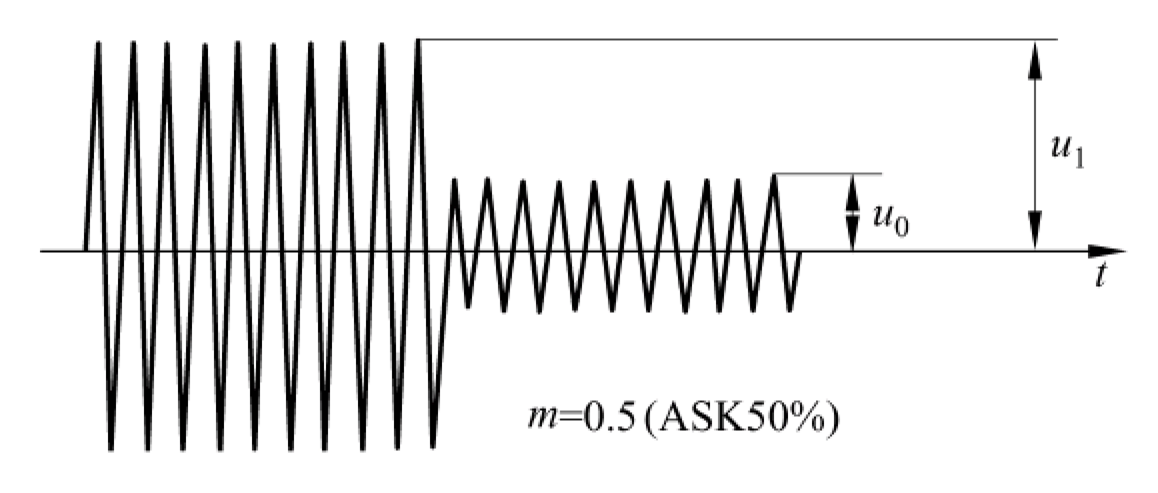


图 8.4　ASK 调制信号

在接收端,当接收到调幅信号时,要予以处理,恢复为数字基带信号,其过程如图 8.5 所示。图中带通滤波器允许指定频段通过,并滤掉输入信号 S_{ASK} 中的噪声。包络检波器输出高频信号的包络,取样脉冲(即同步信号)通过取样判决器将 b 端信号转换成数字基带信号 $S(t)$输出。

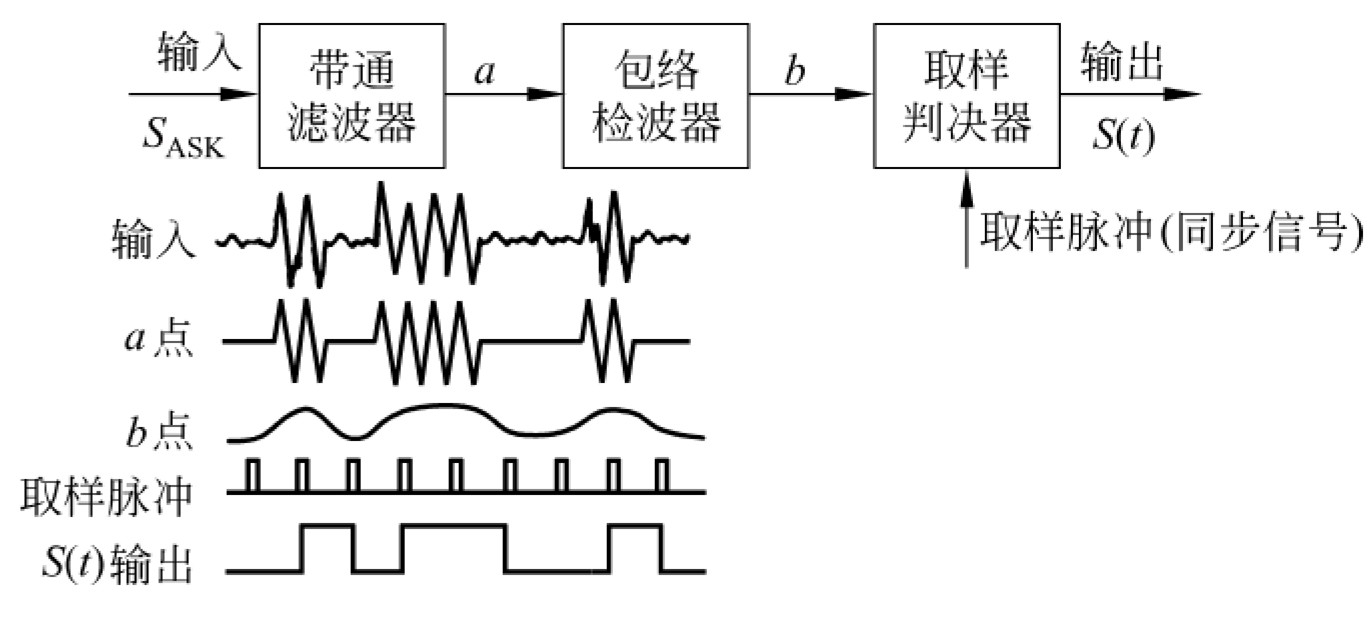
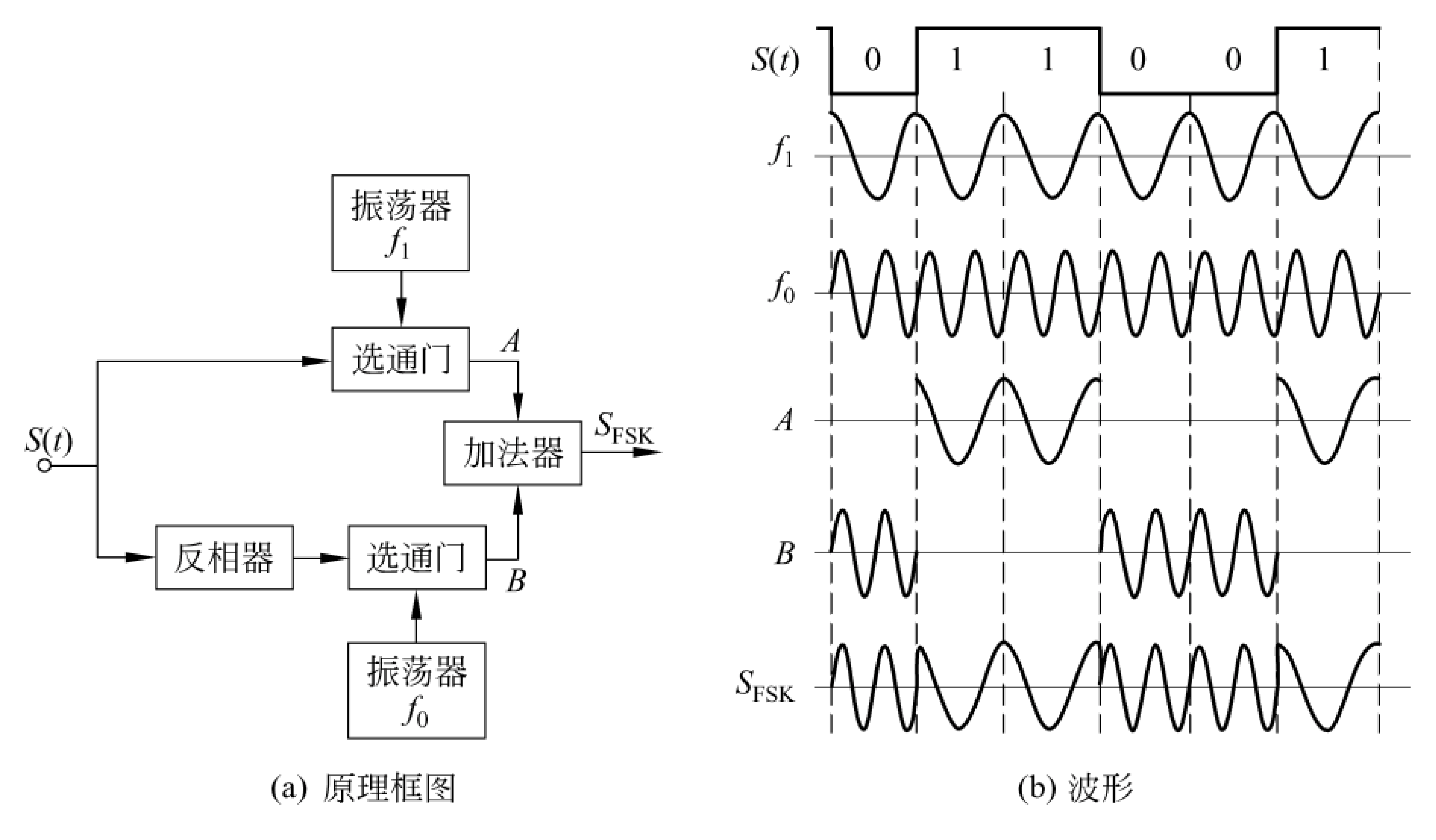


图 8.5　ASK 信号解调器及工作波形

2. 频移键控

图 8.6 所示为 FSK 电路的原理框图和波形,在该图中假设信号 0 的频率为 f_0,信号 1 的频率为 f_1,$f_0=2f_1$。图中的振荡器可以是不要外信号激励的自激振荡器。振荡电路

中有三极管、电感电容、正反馈电路、选频电路等。在加电瞬间，由于三极管之间的参数不会完全相同，在运行状态变化下，再加上正反馈的作用，从而产生振荡，自动将直流电能转化为频率为 f_0 和 f_1 的正弦波。



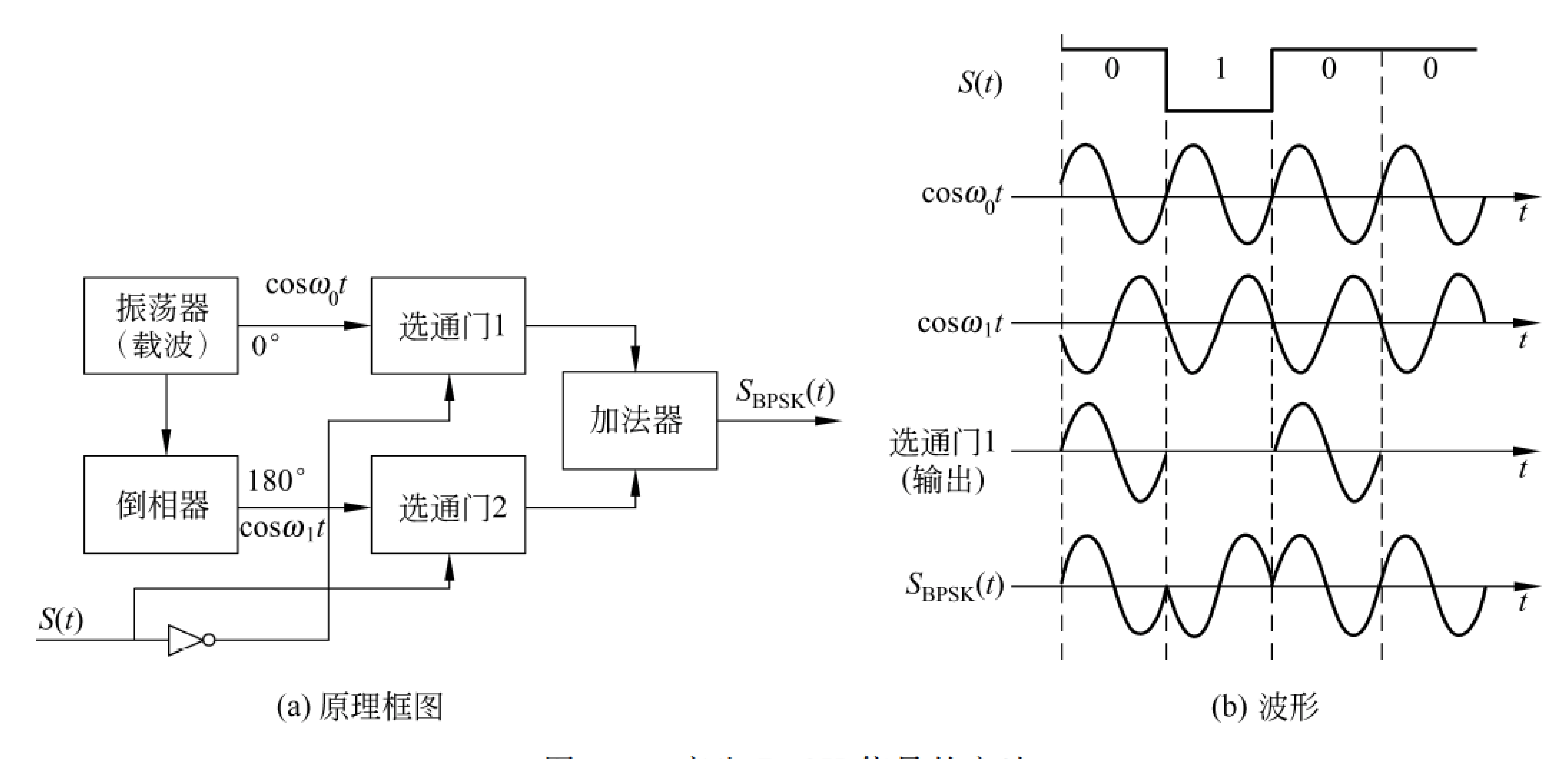
(a) 原理框图 (b) 波形

图 8.6 频移键控(调制)原理框图及其波形

3. 相移键控

用相位偏差 180°的载波，分别表示数字基带信号的 0 和 1。通过对接收信号相位与基准相位的比较，实现解调。此方法称为二进制 PSK(Binary Phase Shift Keying，BPSK)或 2 相 PSK。

如图 8.7(a)所示，倒相器将载波的相位偏移 180°，用数字基带信号 $S(t)$控制门电路，通过加法器得到 BPSK 信号(或称为 2PSK 信号)。图 8.7(b)中的 $\cos\omega_0 t$ 是选通门 1 的输入信号。



(a) 原理框图 (b) 波形

图 8.7 产生 BPSK 信号的方法

解调过程如图 8.8 所示。BPSK 信号经带通滤波器滤掉噪声后,在模拟乘法器中与基准载波相乘(如果两者同相,输出正信号;如果两者异相,输出负信号)。再由包络检波器输出信号的包络到判决器,在取样脉冲的作用下,由判决器输出解调后的数字基带信号。

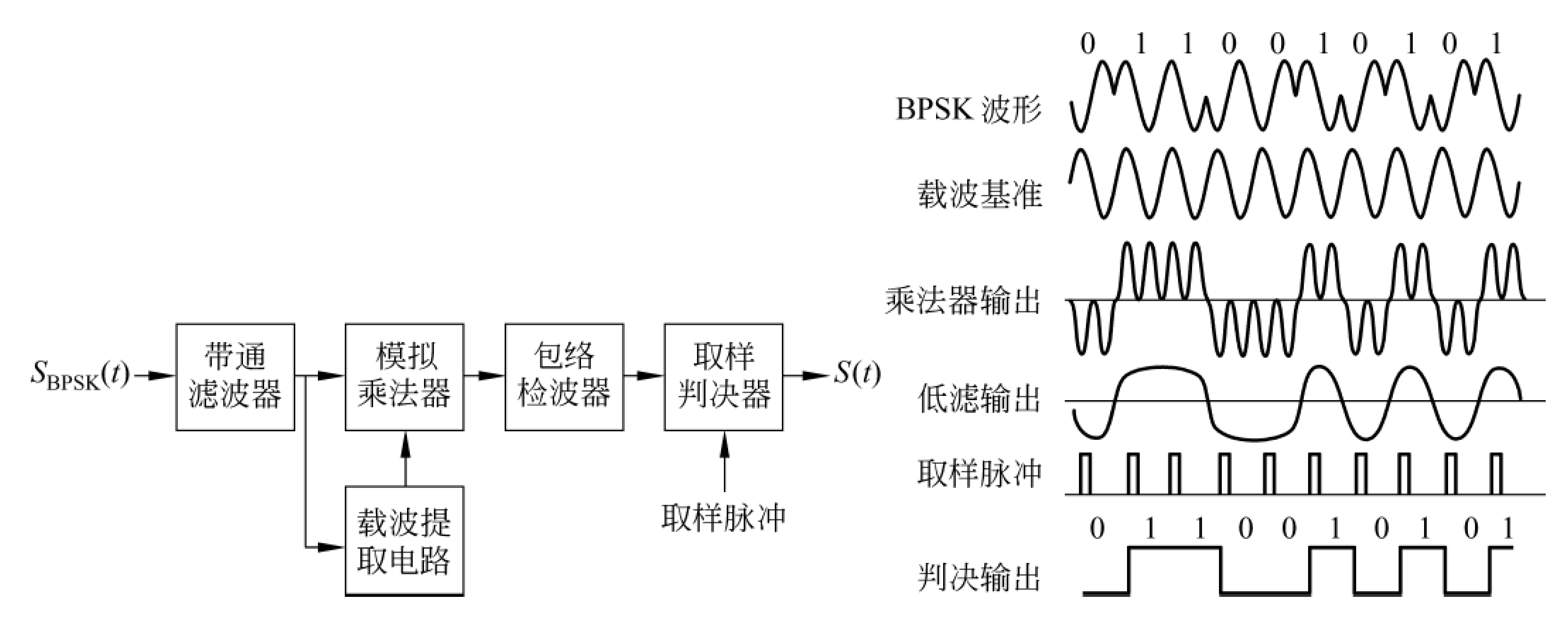


图 8.8　BPSK 信号的解调

4 相 PSK(QPSK)利用载波的 4 种不同相位(45°、135°、225°、275°)表示输入的 2 位数字(00、01、10、11)。

以上介绍了 ASK、FSK 和 PSK 3 种调制方法。请注意编码方式和调制方式的概念是不同的。

8.2.4　负载调制和反向散射调制

读写器与 IC 卡之间的射频信号有两种耦合方式:电感耦合和电磁反向散射耦合。

(1) 电感耦合。根据电磁场基本理论,当射频信号加载到天线之后,在紧邻天线的空间区域内,其电场与磁场之间的转换类似于变压器中电场与磁场之间的转换,称为电感耦合方式(闭合磁路)。该区域的边界为 $\lambda/2\pi$,λ 为波长($\lambda=(3\times10^8\text{m})/f$,$f$ 为频率)。在该区域内其磁场强度随离开天线的距离迅速减小,非接触式 IC 卡的载波频率为 13.56MHz,$\lambda=(3\times10^8\text{m})/13.56\times10^6=22.1\text{m}$,典型的工作距离仅为若干厘米。

(2) 电磁反向散射耦合。当读写器和 IC 卡之间的工作距离增大时(典型距离为 1～10m),一般使用超高频或微波频段的载波。例如,2.45GHz 的微波波长 λ 为 12.2cm,此时读写器与 IC 卡天线之间的通信是通过电磁波的发射与反射而实现的反向散射耦合(雷达原理)。

针对上述两种耦合方式而采用的两种调制方法为负载调制和反向散射调制。

首先介绍一下谐振的概念。

1. 谐振

物理学中的系统共振。当外加动力的频率和系统的固有频率相等时,系统产生极大的振动,振幅比其他情况大很多,称为共振现象。在电路中,当电路中的激励频率等于电路的固有频率时,电路的电磁振荡振幅达到峰值。这种现象称为谐振。

所谓谐振电路,是由电感 L 和电容 C 组成的,可在一个或若干个频率上产生谐振现

象，可从杂乱的电信号中选出所需频率的电信号，并将不需要的电信号加以抑制或滤除。

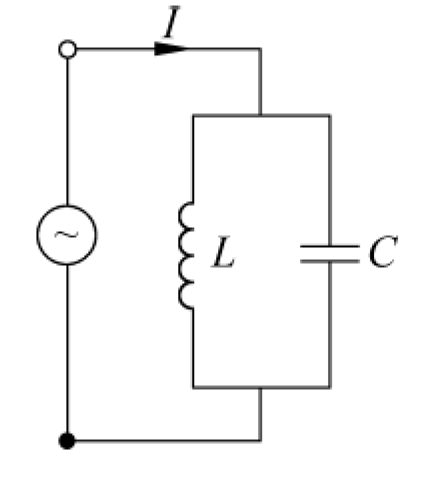


图 8.9　并联谐振

有并联谐振和串联谐振两种情况。

(1) 并联谐振。外加正弦电压，电感 L 与电容 C 并联。谐振时，L 和 C 上的电压达到“无穷大”，电源电压与电流 I 同相位，电源能量由内阻消耗，I 值很小，而元件 L 和电容 C 中流过很大电流。图 8.9 所示为并联谐振电路。

(2) 串联谐振。由电感 L 和电容 C 串联组成的谐振电路，电路达到谐振的条件时，$\omega L-\frac{1}{\omega C}=0$。电路固有的谐振频率 $f=\frac{1}{2\pi\sqrt{LC}}$，$\omega=2\pi f=\frac{1}{\sqrt{LC}}$。元件 L 和电容 C 上的电压都很大，但极性相反，所以串联后对电源来说阻抗很小，电流达到最大值。

2. 负载调制(电感耦合)

如果将一个谐振频率与读写器发送频率相同的 IC 卡放入读写器天线的交变磁场中，IC 卡就能从磁场取得能量，这将导致读写器天线电流的增加和读写器内阻 R_i 上的压降增大，如图 8.10 所示。IC 卡天线上负载(图中的 T)的接通和断开会使读写器天线上的电压发生变化，如果用 IC 卡要发送的数据(基带信号)来控制负载的接通和断开，那么这些数据就能从卡传输到读写器(在读写器天线上测到)，这种数据传送方式称为负载调制。在图 8.10 中，采用的是使用副载波的负载调制。

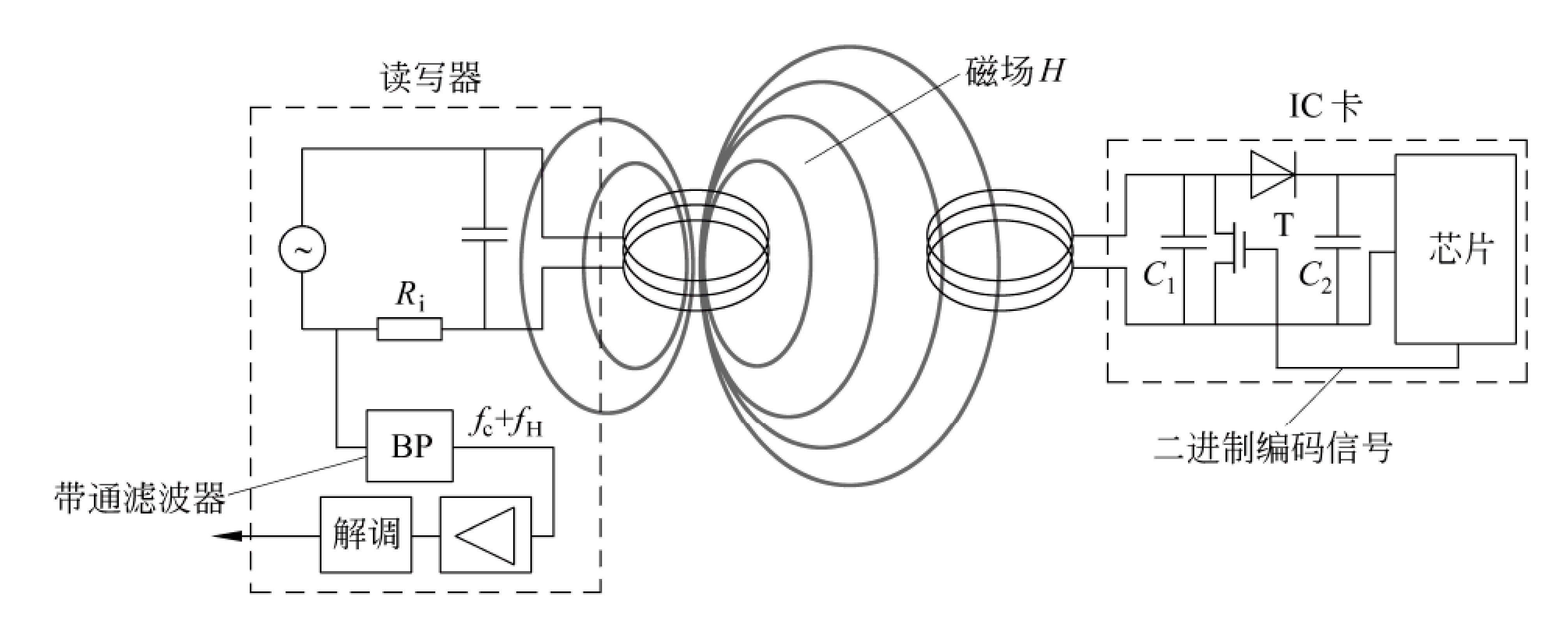


图 8.10　IC 卡能量的获得与负载调制

在卡中，将接收到的载波进行分频而得到副载波。假设载波频率为 13.56MHz，16 分频得副载波，其频率 f_H 为 847kHz(13.56MHz/16)，卡要发送的数据采用曼彻斯特编码，ASK 调制，传输率为 106Kb/s(847/8)，负载调制的过程如图 8.11 所示。用已调制的副载波控制负载开关的接通和断开，对载波实行调制，形成最终的输出。

从图 8.10 中可以看到，IC 卡的能量来自读写器发送的载波，因此在设计读写器数据的编码和调制方式时，要尽量保证不间断地供给能量。

3. 反向散射调制

超高频以上的 RFID 系统采用反向散射调制技术，类似于雷达技术，雷达天线发射的电磁波部分被目标(电子标签)吸收，其他部分向各方散射，其中仅有小部分返回天线。在

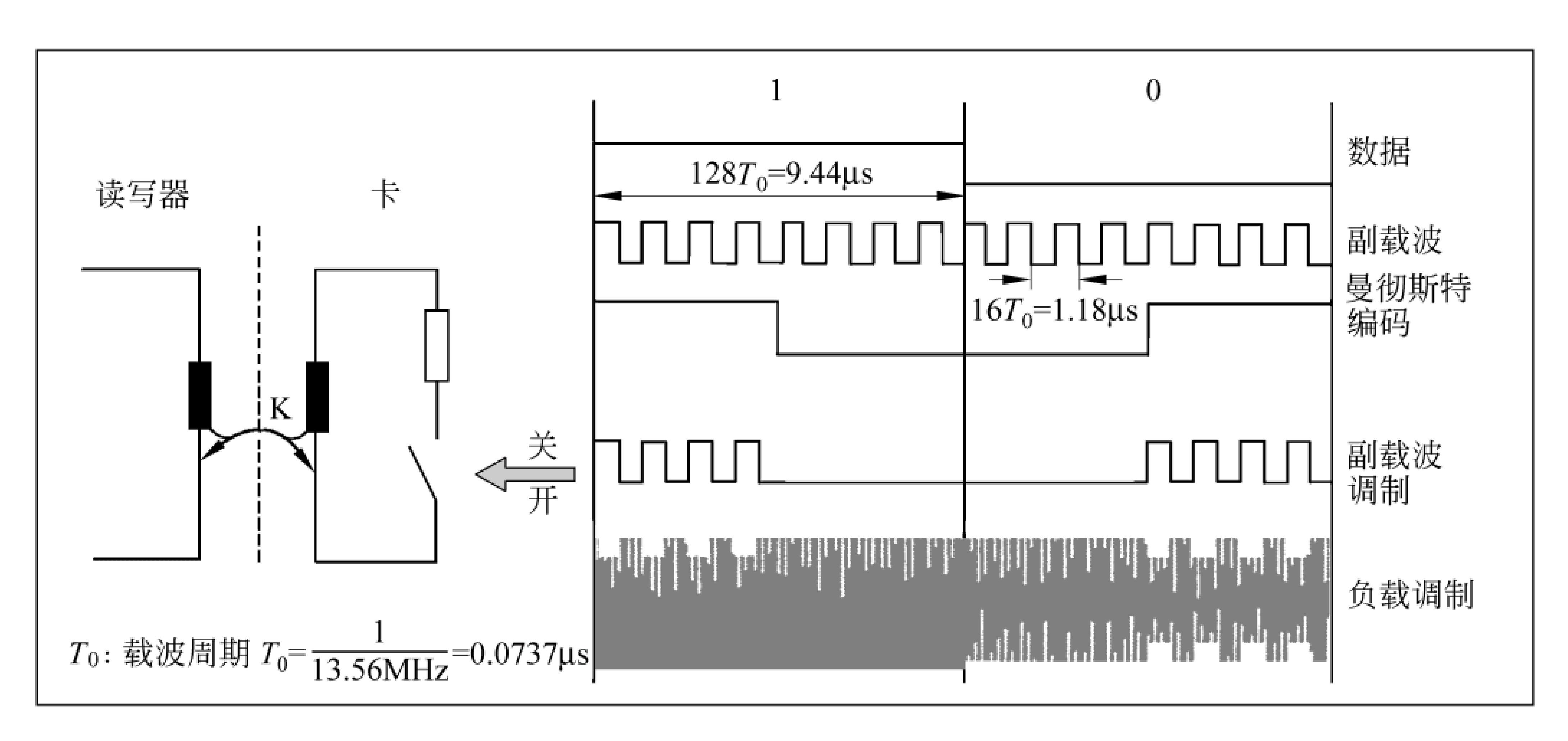


图 8.11　负载调制原理

RFID 系统的电子标签中,通过发送数据控制标签天线的阻抗匹配情况来改变天线的反射系数。在图 8.12 中,要发送的数据是具有两种电平的信号,通过一个简单的混频器(选通门)与中频信号完成调制,调制结果控制阻抗开关,由阻抗开关改变天线的反射系数,从而对载波信号完成调制。这种数据调制方式与普通的数据通信方式有较大的区别,在通信双方,仅存在一个发射机,却完成了双向的数据通信。例如,当标签发送的数据为 0 时,天线开关打开,标签天线处于失配状态,辐射到标签的电磁能量大部分被反射回读写器;当发送的数据为 1 时,天线开关关闭,标签天线处于匹配状态,辐射到标签天线的电磁能量大部分被标签吸收,极少反射回读写器,由此将标签中的数据传送到读写器。

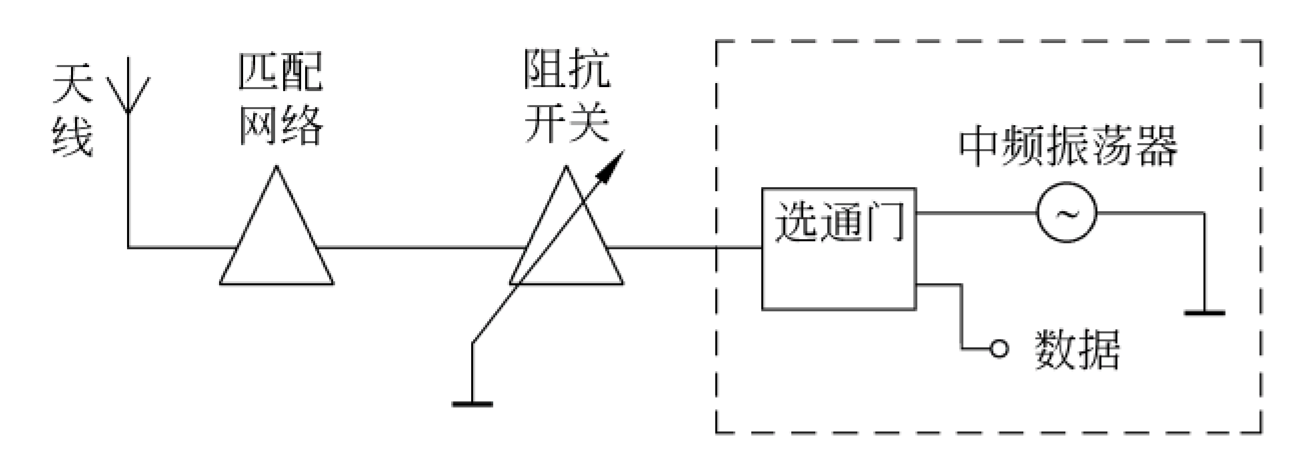


图 8.12　电子标签阻抗控制方式

8.2.5　表面声波电子标签的识别

表面声波(Surface Acoustic Wave, SAW)元件是以压电效应和与表面弹性相关的低速传播的声波为基础的装置,通常工作于 2.45GHz 频率。表面声波电子标签的基本结构如图 8.13 所示。从天线接收到的射频脉冲,经过数字转换器(指状电极结构)转换成表面声波,在压电晶体基片上低速传送(反射)。约经过 1.5ms 的滞后时间,传送到数字转换器将声波转换为电磁波送到天线。在压电晶体基片上完成低速传送功能部分称为反射器,如果将反射器按某种特定的规律设计,使其反射信号表示出特定的编码信息,那么阅读器接收到的反射电脉冲串(响应信号)就是贴有电子标签的物品的特定编码信息,不同物品的反射器都不相同,即可达到自动识别物品的目的。

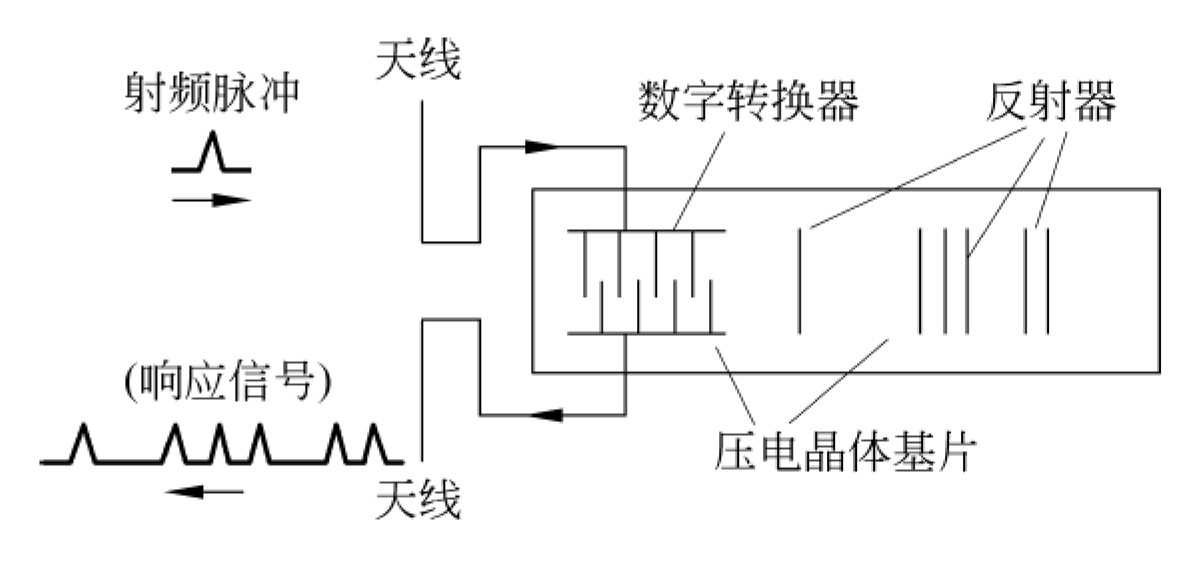


图 8.13　表面声波电子标签

在图 8.13 中，从天线输入一个脉冲，经过反射器得到 6 个脉冲的响应信号。

8.3　扩频技术

1. 扩频

扩频(Spread Spectrum，SS)是用于传输模拟和数字信号的通信技术。图 8.14 举例描述了通用扩频系统的工作过程，发送方输入的数据经过调制器转换成模拟信号，该模拟信号围绕某个中心频率具有相对较窄的带宽，该调制器又可称为信道编码器。然后模拟信号与伪随机数生成器经调制后生成的扩频码同时送到混频器，混频器输出信号的带宽显著增加，即扩展了频谱，并送到天线，通过空中信道进行发送。接收方通过天线接收信号后，将伪随机数生成的同一扩频码同时送到混频器，经解调器后的输出数据即恢复成原发送方的输入数据。

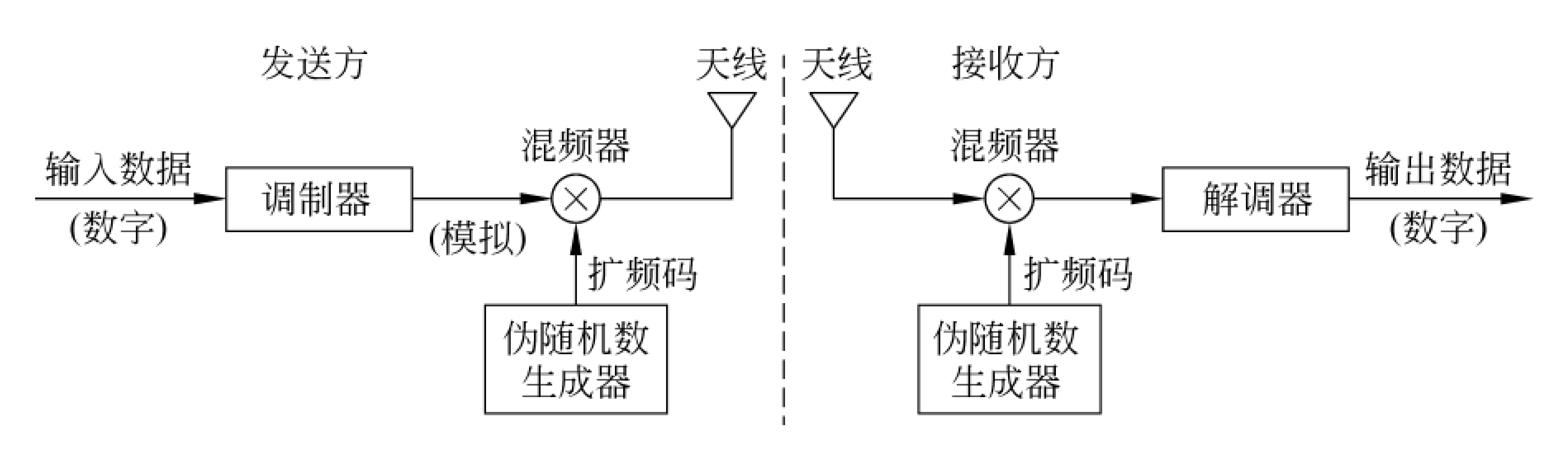


图 8.14　扩频系统的工作过程

以上扩频方法的优点：可防止被窃听与干扰，因为接收方和发送方使用同一扩频码才能恢复原始信息，而且生成扩频码的伪随机数，外人不可得知。

混频器将信号频率由一个量值变换成另一量值，其输出信号频率可以等于两个输入信号之和、差或其他组合电路(非线性元件或选频回路)构成的频率。

目前占主流的扩频技术是下面介绍的跳频扩频和直接序列扩频。本书第 9 章的空中接口标准中用到此项技术。

2. 跳频扩频

用多个扩频码组成一个序列，在时间上按顺序进行频移键控(FSK)调制，产生相应的载波频率，造成载波频率不断跳变，称为跳频。

假设传送数据采用 8 信道跳频扩频(Frequency Hopping SS，FHSS)技术，每一信道分

配的载波频率分别为 f_1、f_2、…、f_8。图 8.15 所示为数据发送时，各数据段与时间间隔和信道的关系。最上面的数据框中的数字表示该段发送时的频率段。例如，最先发送的数据段频率 f_5，在第 1 时间间隔内进行，在图中以最左面的小方块表示。该数据发送总共需要 8 个时间间隔，每一时间间隔工作于某一信道上，即某一频段上。在 IEEE 802.11 的局域网标准中，将时间间隔定义为 300ms。据报道，跳频的频率数(即信道数)可达几十个到几百个。

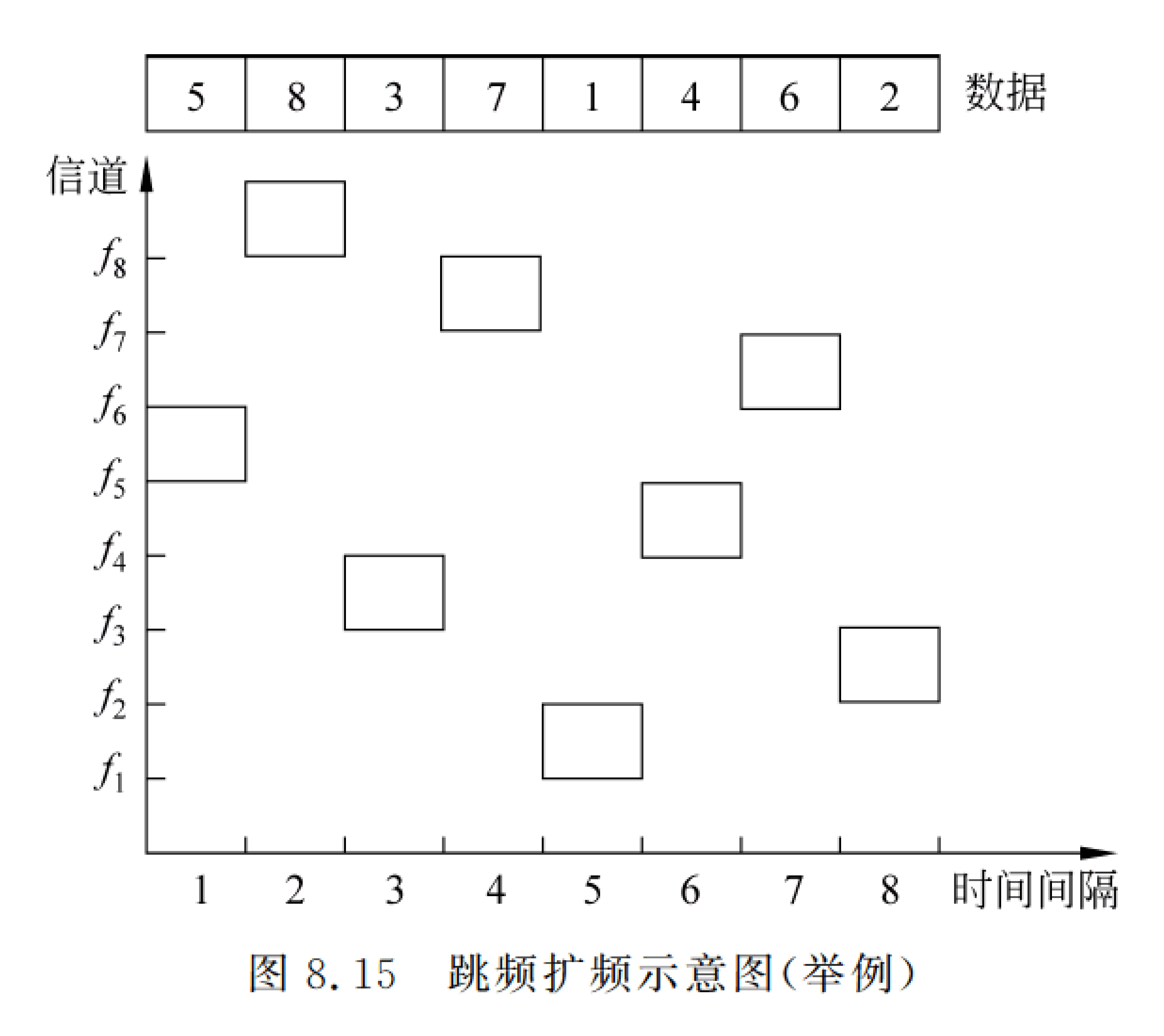


图 8.15　跳频扩频示意图(举例)

3. 直接序列扩频

在直接序列扩频(Direct Sequence SS，DSSS)系统中，输入数据中的每一位(1 或 0)在传输信号中用多位代码表示。例如，数字“0”用 110011 替代，“1”用 000111 替代，其中替代的多位代码称为码片(Chips)，上例有 6 位代码。这种扩展编码能将信号扩展到更宽的频带范围内。在不同的应用例子中，码片的表示形式(如位数等)不是唯一的。

8.4　多路存取(多标签射频识别)

在读写器的作用范围内可能会有多个 RFID 标签存在。在多个读写器和多个标签的射频识别系统中，存在着两种冲突形式：①一个标签同时收到几个读写器发出的命令；②读写器同时收到多个标签返回的信号。当前在射频识别系统中，主要存在第②种识别形式。但有些处理非接触式 IC 卡系统中，仅存在一个读写器和一张 IC 卡之间传送信息的状况，这就不存在多标签识别问题。

在由一个读写器和多个射频标签组成的系统中，存在从读写器到多个射频标签的通信和从射频识别标签到读写器的通信两种基本形式。

在读写器的作用下有多个标签同时将信息传送到读写器，这种方式称为多路存取，如图 8.16 所示。

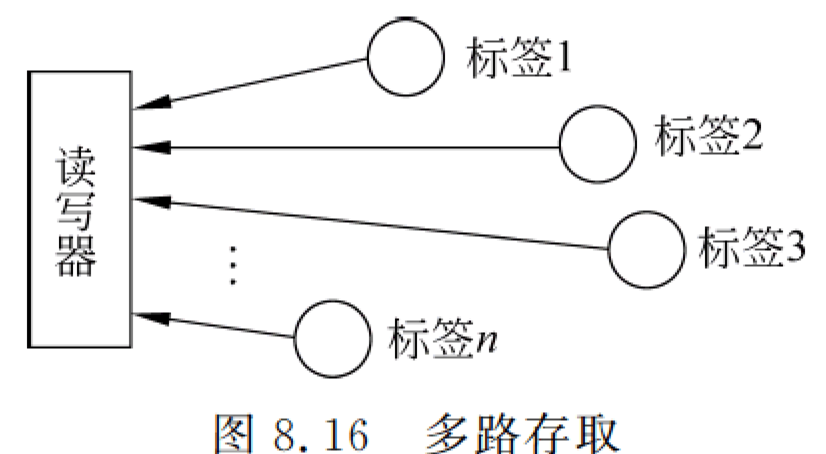


图 8.16　多路存取

多路存取一般有以下几种形式：空分多址、时分

多址和频分多址等。

1）空分多址（Space Division Multiple Access，SDMA）

SDMA 利用不同标签的空间特征（如位置）区分标签，配合电磁波传播的特征，可使不同位置的标签使用相同频率且互不干扰。例如，可利用定向天线或窄波束天线，使电磁波按一定方向发射，且局限在波束范围内，也可控制发射功率，使电磁波只作用在有限距离内。但空间分隔不能太细，某一空间范围一般不会仅有一个标签，所以 SDMA 常与其他多址方式结合使用。

2）频分多址（Frequency Division Multiple Access，FDMA）

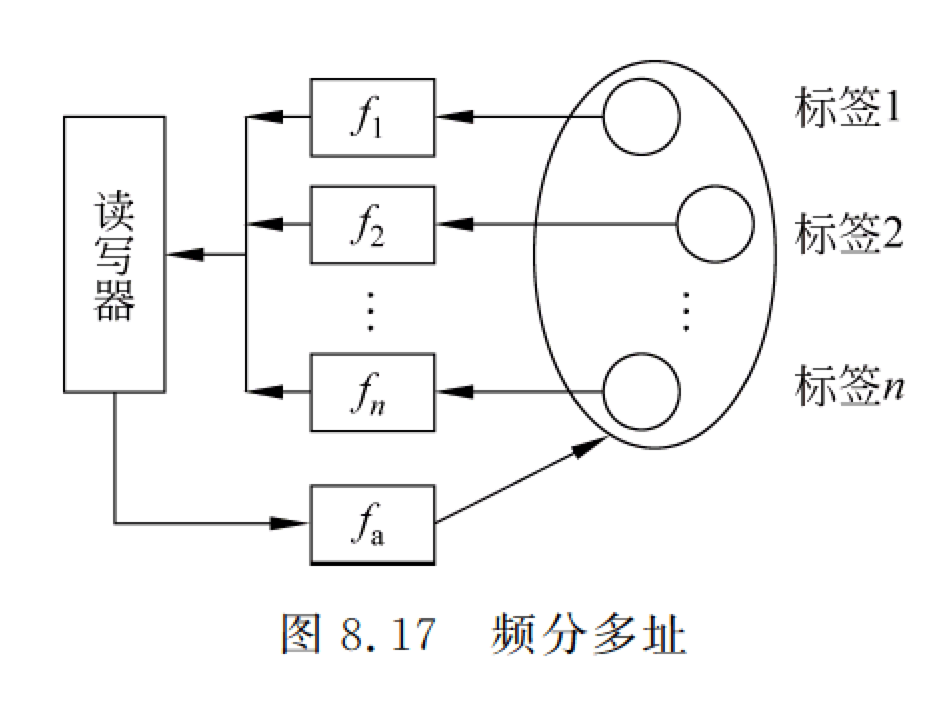


图 8.17　频分多址

FDMA 是把若干个不同载波频率的传输通路同时供标签使用，一般情况下，从读写器到标签的频率 f_a 是固定的，而射频标签可采用不同频率进行数据传送（f_1、f_2、…、f_n），如图 8.17 所示。

3）时分多址（Time Division Multiple Access，TDMA）

TDMA 将整个可用的时间分配给多个标签，构成了多标签防冲突算法中应用最广的一种算法。

TDMA 将数据传送时间划分成若干时隙，每个标签使用某一指定时隙接收和发送信号。各标签按序占用不同时隙，但占用同一频带。TDMA 的主要问题是整个系统要精确同步，各时隙之间应留有保护间隙，以减少数据串扰。

8.5　无线局域网

无线局域网（Wireless Local Area Network，WLAN）是计算机网络与无线通信技术相结合的产物，也是物联网的产生、发展和应用的基础。WLAN 能在几十米到几千米范围内应用。下面讲述 IEEE 802.11 国际标准和蓝牙无线网。与物联网有关的无线局域网、传感网等在第 12 章介绍。

8.5.1　IEEE 802.11 体系结构

WLAN 的基本构成单元称为基本服务集（Basic Service Set，BSS）。它由争用同一共享介质的站点组成。BSS 可以是独立的，也可通过访问点连接到有线 LAN 后，再连接到服务器，构成扩展的服务集（ESS），如图 8.18 所示。

基于流动性，WLAN 定义了以下 3 种站点。

（1）不迁移。站点位置固定或仅在某一个 BSS 内移动。

（2）BSS 间迁移。站点从某一 ESS 的 BSS 中迁移到同一 ESS 的另一个 BSS 中。

（3）ESS 间迁移。站点从某个 ESS 的 BSS 中迁移到另一 ESS 的 BSS 中，在这种情况下，服务可能受到破坏。

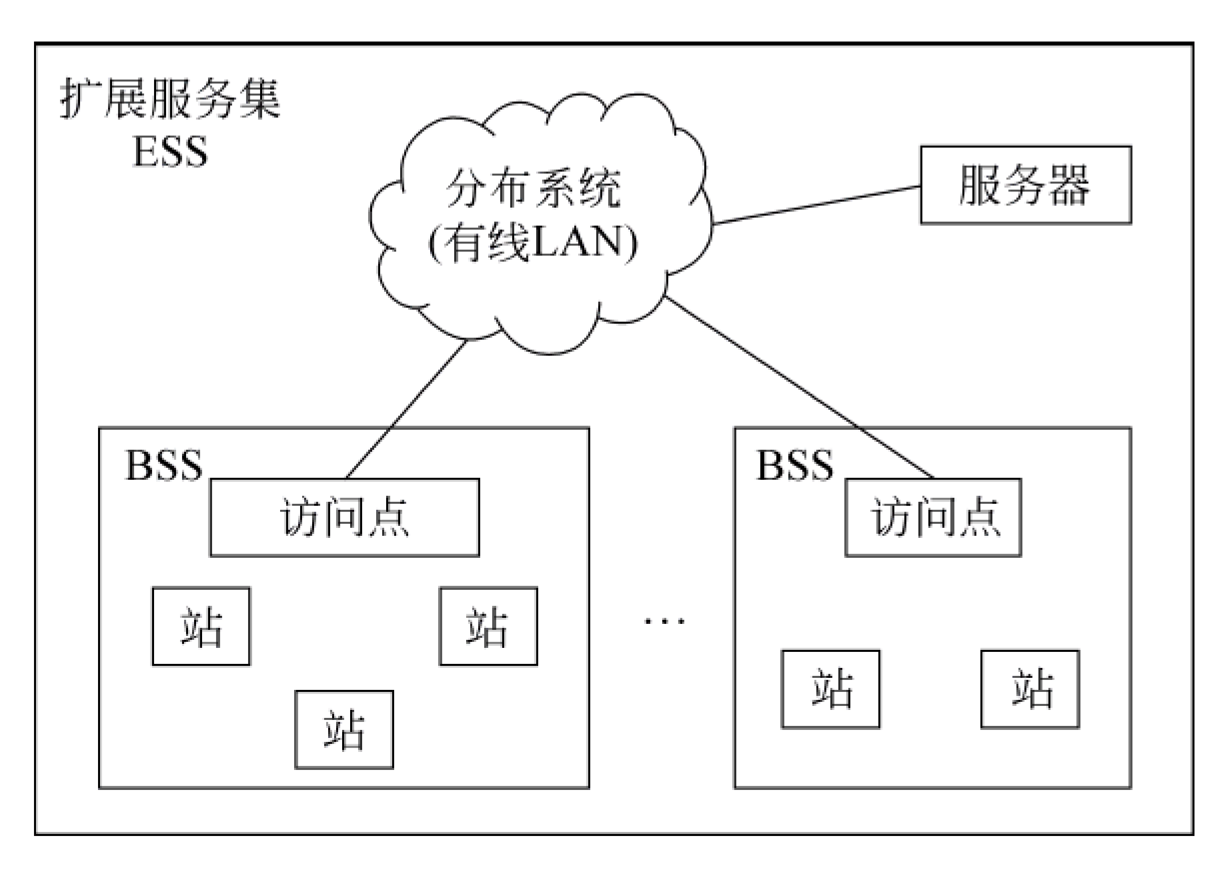


图 8.18　IEEE 802.11 体系结构

8.5.2　ISM 频段和无线网(WiFi、蓝牙和 ZigBee)

1. ISM

国际电信联盟(International Telecommunication Union, ITU)为工业、科学、医疗(Industrial Scientific Medical, ISM)领域分配了无须授权即可使用的频率范围,如表 8.1 所示,发射功率小于 1W。IEEE 802.11 标准和 RFID 标签产品基本上包含在此范围内。

表 8.1　ISM 频谱

频率范围/MHz	中心频率/MHz	频率范围/GHz	中心频率/GHz
6.765～6.795	6.780	2.4～2.5	2.450
13.553～13.567	13.56	5.725～5.875	5.800
26.957～27.283	27.12	24～24.25	24.125
40.16～41.2	40.68	61～61.5	61.25
433.05～434.79	433.92	122～123	122.5
902～928	915	244～246	245

2. 无线网(WiFi、蓝牙和 ZigBee)

1) WiFi(无线局域网)

WiFi 属于在办公室、公共场所和家庭中使用的短距离无线技术,是无线局域网联盟的一个商标,能方便地与现有以太网整合,并接入互联网。

WiFi 的使用频率为 2.450GHz 和 5.800GHz。

IEEE 802.11 b/g/h 定义 WiFi 工作在 2.4G～2.5GHz,被划分成 14 个交叠的、错列的 20MHz 带宽的无线载波信道,各个信道的中心频率之间相差 5MHz(前 13 个频道),第 14 频道的中心频率大些,各信道的中心频率(MHz)如下:

	2412	2417	2422	2427	…	2467	2472	2484	
第	1	2	3	4		12	13	14	信道

例如第 2 信道的中心频率为 2417MHz,其工作范围在 2407～2427MHz。第 3 信道的中心频率为 2422MHz,其工作范围为 2412～2432MHz。

IEEE 802.11a 定义 WiFi 工作在 5.15～5.85GHz，其中，中国为 5.725～5.850GHz，美国为 5.15～5.35GHz 和 5.725～5.825GHz，欧洲为 5.15～5.25GHz，日本为 5.15～5.25GHz，韩国为 5.15～5.35GHz 和 5.46～5.825GHz。

IEEE 802.11b/g/h 不需要许可证，802.11a 则需申请许可证。

2）蓝牙（bluetooth）

蓝牙是一种无线局域网技术，用于连接在 10m 范围内的设备，如笔记本、照相机、打印机、传感器和移动设备等。

当今蓝牙技术实施的协议由 IEEE 802.15 标准定义。蓝牙设备内有短距离无线电发送器，数据传输率为 1Mb/s，频宽为 2.45GHz，有可能在 IEEE 802.11b 的无线局域网和蓝牙局域网之间相互连接。

蓝牙在物理层使用跳频扩频技术，1s 跳频 1600 次，即每个设备在 1s 内可改变 1600 次调制频率，即在跳到其他频率前，一个设备使用该频率的时间仅 625μs。蓝牙使用 FSK 调制，FSK 有一个载波频率，频率偏移在载波频率之上的信息为“1”，在载波频率之下为“0”。

蓝牙在 2.45GHz 频带范围内分成 79 个通道，每个通道的频率偏移值为 1MHz，每个通道的载波频率定义为

$$f_c = (2404 + n)\text{MHz}$$

式中，$n=0,1,2,\cdots,78$。

蓝牙支持“点到点”和“点到多点”的连接。

3）ZigBee 技术

ZigBee 是近距离、低速率、低功耗、低复杂度、低成本和高可靠性的双向无线数据传送技术。遵循 IEEE 802.15.4 协议，是一个由多个到 65 000 个无线数据节点组成的网络，主要是为工业现场自动化控制数据传送而建立的。例如，其所连接的传感器不仅可以直接进行数据采集和监控，而且还可以自动中转别的网络节点传过来的数据资料。

ZigBee 联盟于 2001 年成立，2004 年发布第一个标准。

3. 无线局域网的特点

WLAN 是在有线局域网基础上发展起来的，摆脱了有线传输介质的束缚，实现了便携式设备的网络接入功能，并可将网络延伸到线缆无法连接的地方，节省了组网的费用。

但是由于无线信道存在各种干扰和噪声，无线电波可能会受到窃听和恶意篡改，从而影响可靠性和安全性。

便携设备要注意节能，从而延长电池使用时间和提高电池寿命。

习题

1. 射频识别系统由哪些部件组成？读写器与 IC 卡之间的射频信号传送归纳为哪两种方式？
2. RFID 标签和非接触式 IC 卡的相同点和区别是什么？
3. 请解释基带、带宽和宽带的含义。

4. 数字信号常用的有哪些编码方式？了解编码和调制两个概念的联系与区别。
5. 常用的调制方式有哪些？调制与解调有什么关系？为什么要对数字信号进行调制？
6. 跳频扩频(FHSS)和直接序列扩频(DSSS)系统的工作原理及其组成是什么？
7. 为什么要讨论多路存取的方法？一般有哪几种方法？
8. 叙述 IEEE 802.11 定义的频谱范围与本章中介绍的射频技术的关系。
9. 国际电信联盟为 ISM 领域分配频率范围的作用是什么？
10. 什么是 WiFi，其作用是什么？
11. 非接触式 IC 卡和 RFID 标签怎样得到工作所需的直流电源？请比较各种方法的优缺点。

第 9 章　非接触式 IC 卡国际标准 ISO/IEC 14443 和 ISO/IEC 15693

9.1　非接触式 IC 卡的种类和能量传送

1. 非接触式 IC 卡的种类

根据非接触式 IC 卡操作时与读写器发射表面距离的不同，定义了 3 种卡及其相应的读写器，如表 9.1 所示。

表 9.1　非接触式 IC 卡、读写器及其对应的国际标准

IC 卡	读写器	国际标准	读写距离/cm
CICC	CCD	ISO/IEC 10536	紧靠（基本淘汰）
PICC	PCD	ISO/IEC 14443	<10
VICC	VCD	ISO/IEC 15693	<50

ICC 为集成电路卡，表 9.1 中 CICC 为 Close-Coupled ICC（紧靠式 IC 卡），PICC 为 Proximity ICC（接近式 IC 卡），VICC 为 Vicinity ICC（邻近式 IC 卡），CD 为 Coupling Device，是读写器中发射电磁波的部分。

与接触式 IC 卡相比，非接触式 IC 卡还需要解决下述 3 个问题。

（1）IC 卡如何取得工作电压。

（2）读写器与 IC 卡之间如何交换信息。

（3）多张卡同时进入读写器发射的能量区域（即发生冲突或称为碰撞）时，如何处理。

2. 能量传送

PCD 产生耦合到 PICC 的 RF 电磁场，用以传送能量和双向通信（经过调制/解调）。

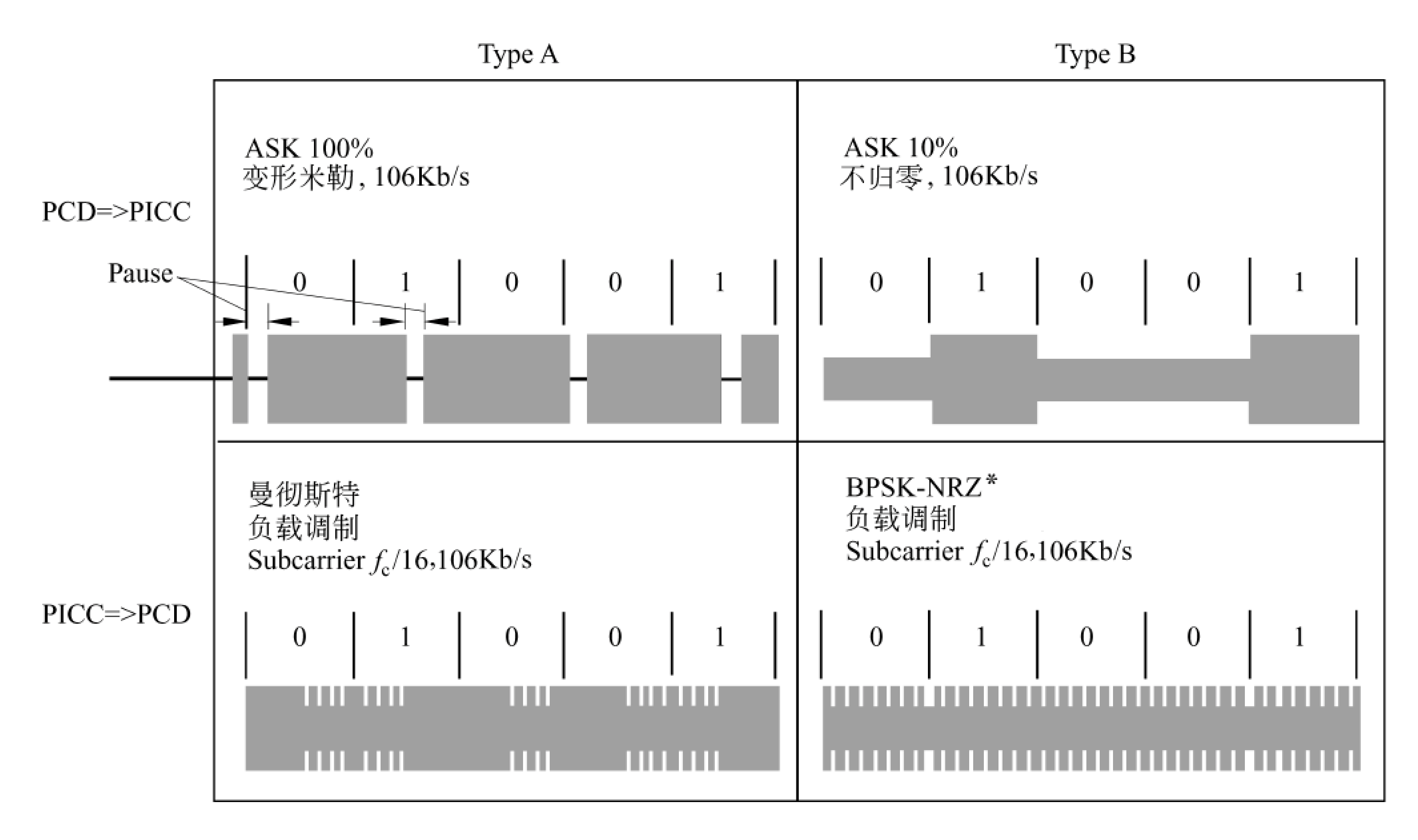
（1）PICC 获得能量后，将其转换成直流电压。

（2）RF 场的载波频率 f_c 为 13.56MHz±7kHz。

（3）RF 场的 H 值（磁场强度）为 1.5～7.5A/m（有效值），在此范围内 PICC 应能不间断地工作。

9.2　ISO/IEC 14443 的信号接口（Type A 和 Type B）

IC 卡与读写器之间规定了两种信号接口：Type A（A 类）和 Type B（B 类）。图 9.1 所示为在 PCD 和 PICC 之间传送二进制信号（01001）的举例。两个方向传送的信号表示形式是不同的。



*注：数据 0 和 1 的相位可能反相(Type B)

图 9.1　Type A 和 Type B 接口通信信号举例

9.2.1　Type A 信号

1. 从 PCD 传送到 PICC 的信号(Type A)

1）传输率

载波频率为 13.56MHz，在初始化和防冲突期间，数据传输率为 13.56MHz/128＝106Kb/s，一位数据所占的时间周期为 9.4μs。

2）调制

采用 ASK 100%调幅制，在 RF 场中创造一个“间隙(Pause)”来传送二进制数据，图中灰影部分为载波，空白处即为间隙。间隙的实际波形如图 9.2 所示。

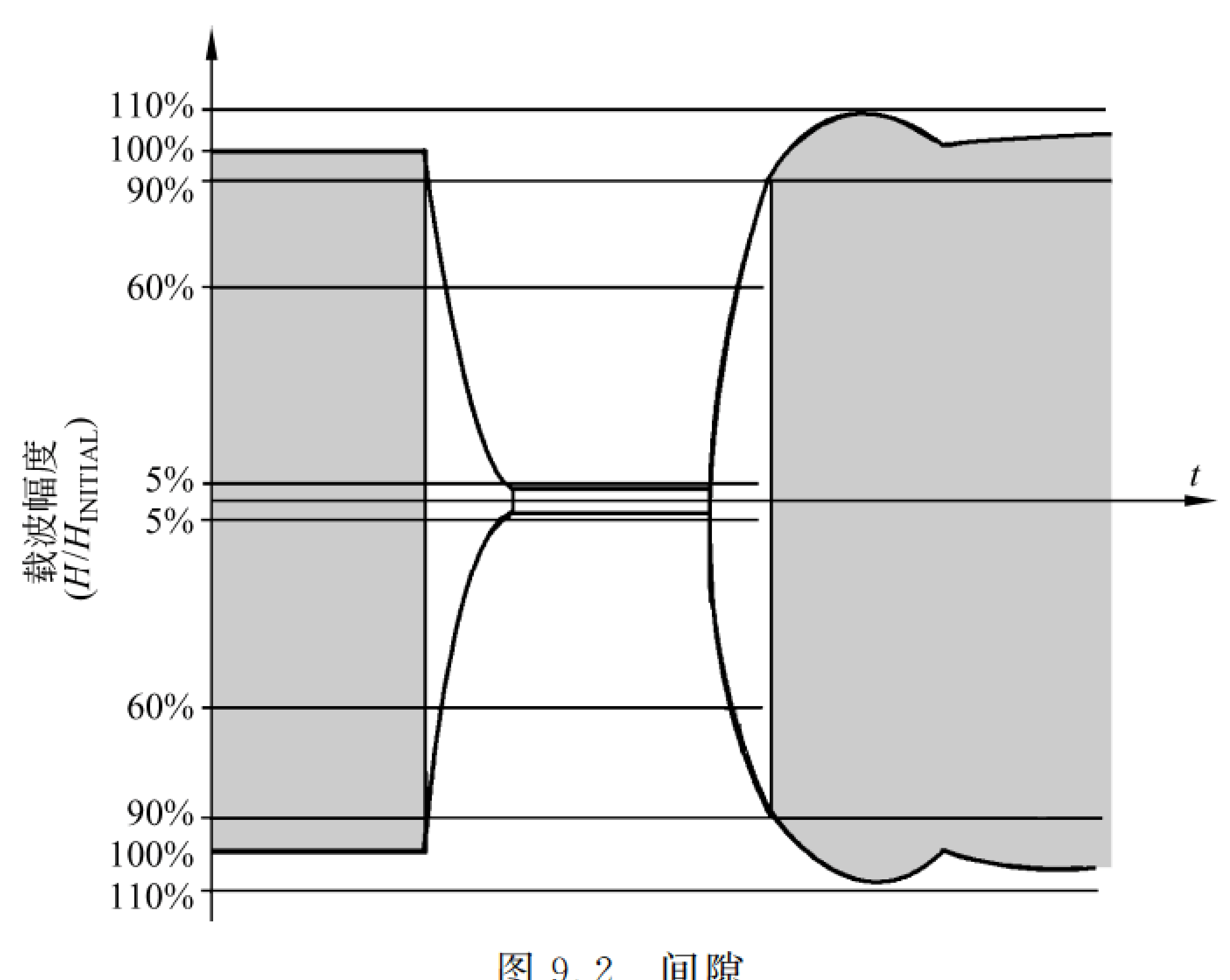


图 9.2　间隙

3）数位的表示和编码

定义以下时序。

（1）位周期的中间产生一个间隙，代表逻辑 1。

（2）在位周期的开始产生一个间隙，代表逻辑 0。

（3）如果在整个位期间（$128/f_c$）不发生调制，其意义如下。

① 假如相邻有两个或更多的 0，则第 1 个 0 不调制，从第 2 个 0 开始（包括其后面的 0）采用上述的逻辑 0。

② 假如有两个或两个以上周期不调制，则表示无信息。

（4）通信开始：逻辑 0。

通信结束：逻辑 0，跟随其后为不调制。

2. 从 PICC 传送到 PCD 的信号（Type A）

1）数据传输率

在初始化和防冲突期间，数据传输率为 $f_c/128$（106Kb/s）。

2）负载调制

PICC 通过电感耦合区与 PCD 进行通信。在 PICC 中，利用 PCD 发射的载波频率生成副载波（频率为 f_s），副载波是在 PICC 中用开通/断开负载的方法（Load Modulation）实现的。

副载波的频率 $f_s=f_c/16$（≈847kHz），在初始化和防冲突期间，一位时间等于 8 个副载波时间。

3）数位表示和编码

采用曼彻斯特编码，定义如下。

（1）载波被副载波在位周期的前半部（50%）调制，表示逻辑 1。

（2）载波被副载波在位周期的后半部（50%）调制，表示逻辑 0。

（3）通信开始（S）：逻辑 1。

（4）通信结束（E）：不被副载波调制。

（5）无信息：在整位周期内载波不被副载波调制。

9.2.2 Type B 信号

1. 从 PCD 传送到 PICC 的信号（Type B）

1）数据传输率

在初始化和防冲突期间，数据传输率为 $f_c/128$（≈106Kb/s）。

2）调制

采用 ASK 10%调幅制（调制指数$=(a-b)/(a+b)=8\%\sim14\%$），其调制波形如图 9.3 所示。

3）数位表示和编码

位编码格式为非归零制 NRZ。

（1）逻辑 1：载波高幅度（无调制）。

（2）逻辑 0：载波低幅度。

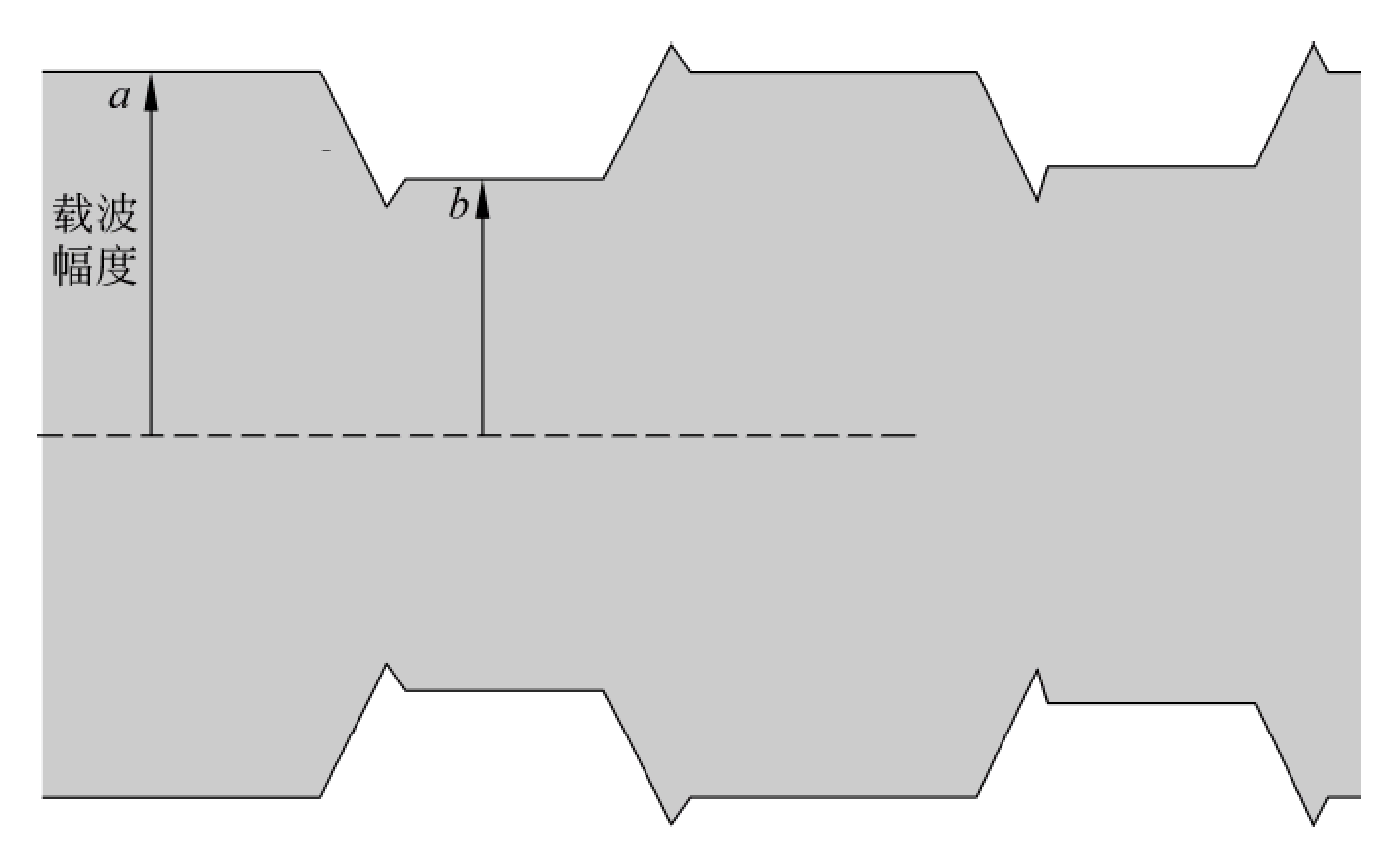


图 9.3　Type B 调制波形

2. 从 PICC 传送到 PCD 的信号(Type B)

1）数据传输率

在初始化和防冲突期间,数据传输率为 $f_c/128$(≈106Kb/s)。

2）负载调制

PICC 通过电感耦合区与 PCD 进行通信,在 PICC 中利用 PCD 发射的载波频率生成副载波(频率为 f_s),副载波是在 PICC 中用开通/断开负载的方法实现的。

副载波的频率 $f_s=f_c/16$(≈847kHz)。在初始化和防冲突期间,一位时间等于 8 个副载波时间。

PICC 仅在数据传送时产生副载波。

3）数位表示和编码

位编码采用不归零制 NZR,逻辑状态的转换用副载波相移 180°来表示。φ_0 表示逻辑 1,$\varphi_0+180°$表示逻辑 0,如图 9.4 所示。逻辑 1 和逻辑 0 可分别定义为二进制数 1 和 0,或数 0 和数 1。

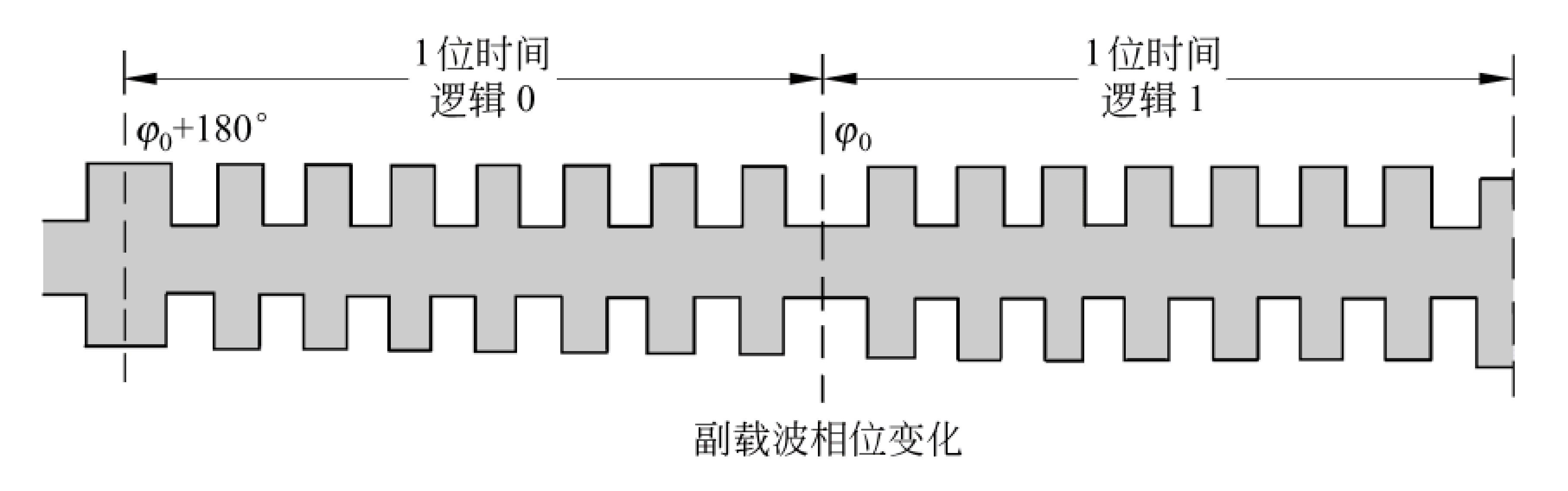


图 9.4　数位表示

从 PCD 发出任一命令后,在 TR0 的保护时间内,PICC 不产生副载波,TR0＞$64/f_s$(64 个载波周期)。

然后,在 TR1 时间内 PICC 产生相位为 φ_0 的副载波(在此期间相位不变),TR1＞$80/f_s$。副载波的初始相位定义为逻辑 1,所以,第一次相位转变表示从逻辑 1 转变到逻辑 0。

TR0 和 TR1 的说明见图 9.8(a)。

9.3 ISO/IEC 14443-3 初始化和防冲突

本部分描述以下内容。

(1) PICC 进入 PCD 场的轮询过程。

(2) 在 PCD 与 PICC 之间进行通信的初始化阶段所用的字节格式、帧和时序。

(3) 初始化 REQ 和 ATQ(命令和应答)的内容。

(4) 在多张卡中检出一张卡并与之通信的方法。

(5) 在 PCD 和 PICC 之间进行初始化通信的其他参数。

(6) 基于应用规范,加速从多张卡中选出一张卡的可选方法。

9.3.1 轮询

为了检出进入 PCD 能量场的 PICC,PCD 重复发出请求命令 REQA/REQB,并查询 PICC 的响应 ATQA/ATQB,这一过程称为轮询(Polling)。

REQA 和 REQB 分别为采用 Type A 和 Type B 规范的 PCD 所发出的请求命令。

当 PICC 进入射频场后,应能在 5ms 时间内接收 PCD 的请求命令。

9.3.2 Type A——初始化和防冲突

本节描述应用于 Type A 的 PICC"位冲突"检测协议。

1. 字节与帧的格式和防冲突原理

命令帧和响应帧应成对传送,PCD 发送帧到 PICC 后,经过延迟时间,PICC 发送帧到 PCD。然后再延迟时间后,可启动下一对帧的传送。

1) 帧延迟时间

帧延迟时间定义为在相反方向上所发送的两个帧之间的时间。

(1) PCD 到 PICC 的帧延迟时间。

PCD 发送命令的最后一个间隙(逻辑 1 或逻辑 0)结束与 PICC 发送响应的起始位的第一个调制边之间的最小时间应遵守图 9.5 中的规定。其中,$1/f_c=73.75$ns。

为适应所有命令的操作,将图 9.5 中的 $1236/f_c$ 修改为 $(n\times128+84)/f_c$,$1172/f_c$ 修改为 $(n\times128+20)/f_c$,其中 $n\geqslant9$,且为整数。当 $n=9$ 时,即为图 9.5 中的时序。

(2) PICC 到 PCD 的帧延迟时间。

PICC 发送的最后一个调制与 PCD 发送的第一个间隙之间的时间,至少为 $1172/f_c$。

2) 请求保护时间

相邻两个 REQA 命令的起始位之间的最小时间定义为请求保护时间,其值为 $7000/f_c$。

3) 帧格式(短帧和标准帧)

(1) 短帧。REQA 命令帧和 WUPA 命令帧。REQA 帧如下。

	LSB						MSB	
S	0	1	1	0	0	1	0	E

发送的
第一位　　'26'

这两帧应用于初始化通信,包含以下内容。

① 通信起始位 S。

② 命令代码 7 位,最低有效位(Least Significant Bit,LSB)先发送,最高有效位(Most Significant Bit,MSB)最后发送。REQA 的命令代码为'26',WUPA 的命令代码为'52'。

③ 通信结束位 E。

无奇偶校验位。

(2) 标准帧。用于数据交换,其组成如下。

① 通信起始位 S。

② $n\times$(8 个数据位+奇校验位),其中 $n\geqslant 1$。数据字节的最低位先发送,每一数据字节后有一奇校验位。

③ 通信结束位 E。

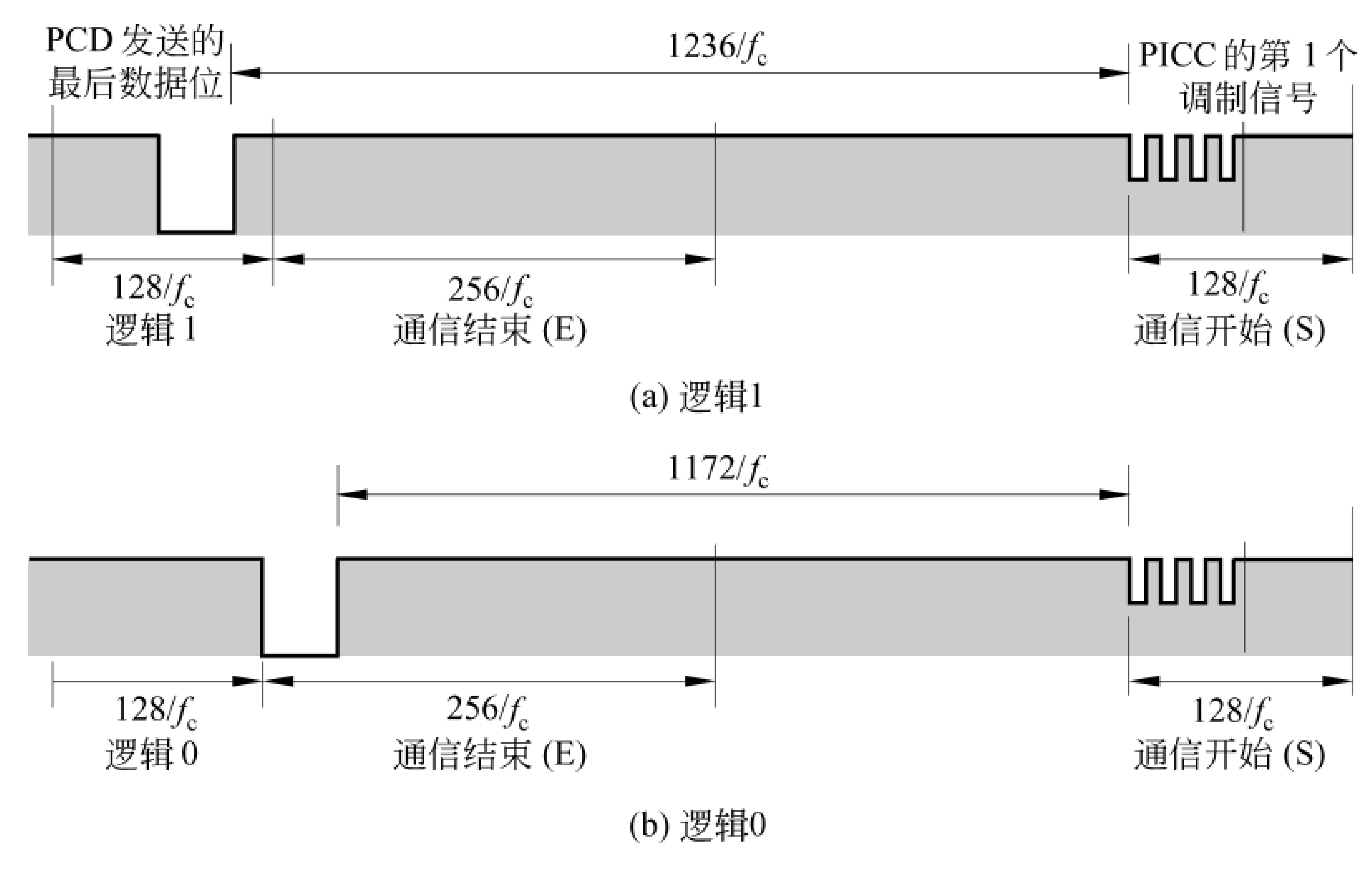


图 9.5　PICC 应答时序

4) 面向位的防冲突帧

当至少有两个 PICC 同步发出不同的唯一标识码 UID 到 PCD 时,PCD 就能检测到冲突,在这种情况下,至少有一位的载波在整个位周期内都被副载波调制。

举例如下(为便于说明,缩短了 UID 的长度)。

假设在 PCD 磁场内有 3 张智能卡,其 UCD 长度为 8 位,分别为:

	第	1	2	3	4	5	6	7	8	位
第 1 张		1	0	0	1	0	1	0	0	
第 2 张		1	0	0	1	1	1	0	0	
第 3 张		1	0	1	0	1	0	1	0	

防冲突的目的是先从3张卡中选出一张卡，根据其UID和应用需求进行操作，完成后，再选出另一张卡进行操作……直到场内3张卡都处理完毕。

防冲突过程(即选卡步骤)如下。

第1步：PCB发出防冲突命令，3张PICC发回各自的UID，PCD接收后，在第3位整个周期内都有副载波调制信号，说明这是冲突位。

第2步：PCD再发出防冲突命令，同时给出被选卡UID的前3位为100，此时将第3张卡封闭，第1张和第2张发回UID，此时在第5位发生冲突，进入第3步(如果前3位选为101，此时立即将第3张选出)。

第3步：PCD再发出防冲突命令，同时给出被选卡UID的前5位为10010，第1张卡发回UID，这就是被选出的卡，UID=10010100。

然后继续进行防冲突，逐次读出第2张、第3张卡的UID(或读出第3张和第2张卡的UID)。

2. PICC的状态及其转换

(1) POWER OFF(断电)状态。PICC由于缺少载波能量而处于断电状态，也不发射副载波，等待电磁场的到来。

(2) IDLE(休闲)状态。电磁场激活后延迟5ms时间以内，PICC进入IDLE状态，在这一状态，PICC加电，同时能够对已被调制的信号解调，并认识来自PCD的命令。

(3) READY(就绪)状态。当接收到一个有效的启动命令，就从休闲状态进入了READY状态，在这一状态中，可采用位帧防冲突或其他可供选择的防冲突方法。当PICC的唯一标识符UID被PCD发来的选择命令选中时，就进入激活状态。

(4) ACTIVE(激活)状态。在激活状态，完成本次应用所要求的全部操作，然后进入停止状态。

注：每张卡都有一标识符(IDentifier，ID)，在同一应用中的所有卡的ID应该是各不相同的(至少有一位不相同)，称之为“唯一标识符(Unique IDentifier，UID)”。

(5) HALT(停止)状态。接收HALT命令的PICC进入HALT状态。

查出磁场内各IC卡标识符不同位值(0，1)位置的方法称为位帧防冲突方法。

3. 命令集

PCD管理进入其能量场的多张卡的命令如下。

- REQA(启动)命令。
- WUPA(唤醒)命令。
- ANTICOLLISION(防冲突)命令。
- SELECT(选择)命令。
- HALT(停止)命令。

所有命令都是由PCD发出的，命令的格式不完全相同。

1) REQA命令和WUPA命令

这两条命令都是使卡进入READY状态，其差别是REQA命令从IDLE状态进入READY状态，而WUPA命令从HALT状态进入READY状态。命令代码如表9.2所示。

当PICC接收到REQA命令或WUPA命令后，在PCD能量场范围内的所有PICC同步发出ATQA响应，指出本卡的UID的长度(4、7或10个字节)和采用位帧防冲突。

UID 的长度可选，可以由 1、2 或 3 个部分组成，用 CL1、CL2 和 CL3 表示，如表 9.3 所示，UID 的最后部分(CLn)都为 4 个字节，而其前面的部分都是 3 个字节。

表 9.2 REQA 和 WUPA 命令代码

b_7	b_6	b_5	b_4	b_3	b_2	b_1	说　明
0	1	0	0	1	1	0	'26'＝REQA
1	0	1	0	0	1	0	'52'＝WUPA
所有其他							专用或 RFU

表 9.3 UID 的长度

UID 长度	最大级联 CL	UID 的字节数
1	CL1	4
2	CL1＋CL2	7(3＋4)
3	CL1＋CL2＋CL3	10(3＋3＋4)

PCD 接收 ATQA 响应，PICC 进入 READY 状态，执行防冲突循环操作。

2) ANTICOLLISION 命令和 SELECT 命令

这两条命令分别用于防冲突循环和防冲突结束，命令格式如下。

SEL	NVB	UID CL_n 数据位	BCC
1 字节	1 字节	0～4 字节	1 字节

(1) 命令代码 SEL(1 字节)，编码如表 9.4 所示。

表 9.4 SEL 的编码

b_8	b_7	b_6	b_5	b_4	b_3	b_2	b_1	说　明
1	0	0	1	0	0	1	1	'93'选择 UID CL1
1	0	0	1	0	1	0	1	'95'选择 UID CL2
1	0	0	1	0	1	1	1	'97'选择 UID CL3

(2) 有效位数量 NVB(1 字节)。

当 NVB＝'70'时，说明 UIDCLn 为 4 个字节，为 SELECT 命令；当 NVB≠'70'时，为 ANTICOLLISION 命令。

PCD 发出防冲突命令的目的，是想从 PICC 得到卡的 UID CL_n 的一部分或全部，从而达到在多张卡中选出一张卡进行交易的目的。

3) HALT 命令

HALT 命令由 4 个字节组成：

'50'	'00'	CRC-A
1B	1B	2B

4. 防冲突和应用程序执行流程

防冲突和应用程序执行流程如图 9.6 所示。如果检查 UID 完整，表示被检出的

PICC 的所有 UID 位已经核实,该卡的防冲突流程已结束。否则循环执行防冲突流程。

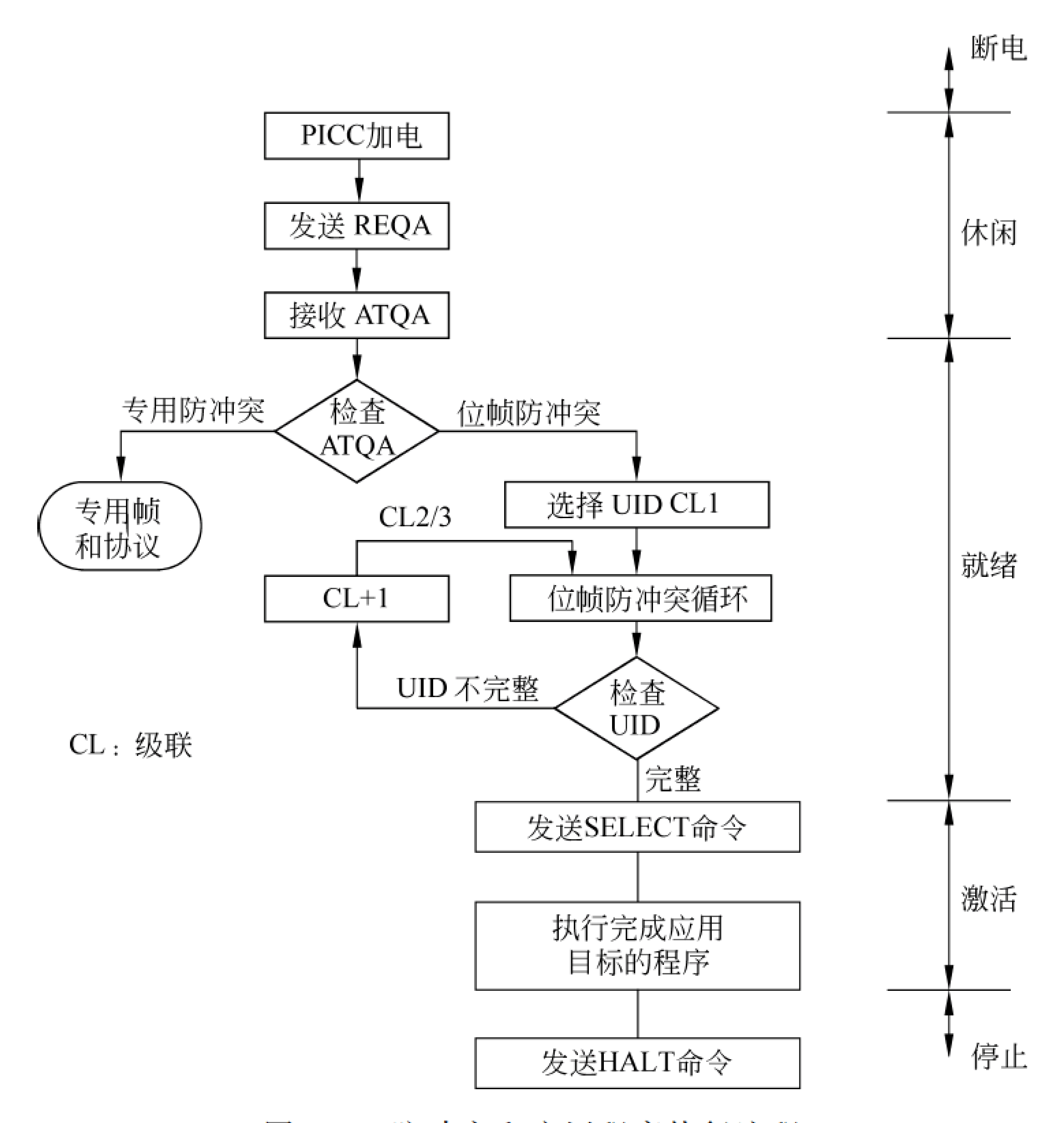


图 9.6 防冲突和应用程序执行流程

9.3.3 Type B——初始化和防冲突

1. 字节和帧

本节描述 Type B PICC 在通信初始化和防冲突阶段的帧和命令的格式。

1) 字节传送格式与字符间隔

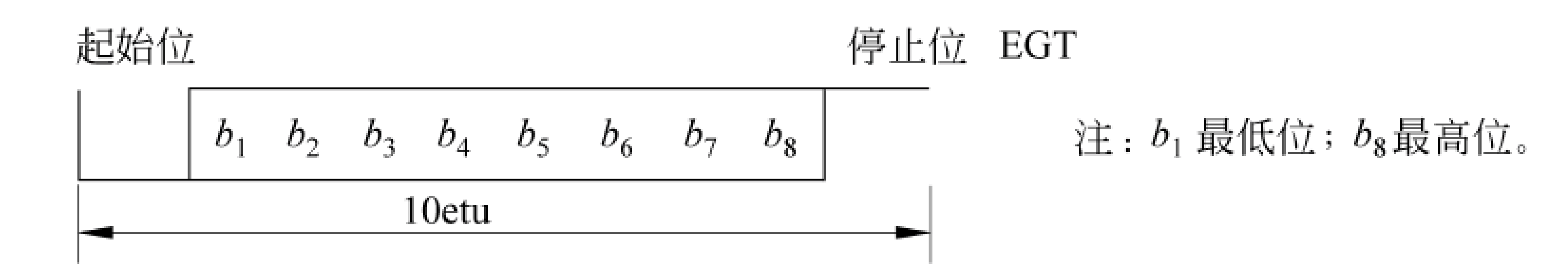
在防冲突顺序中,PICC 和 PCD 之间双向传送的数据字节格式包括如下部分。

(1) 1 个低电平起始位。

(2) 8 个最低位先发送的数据位。

(3) 1 个高电平停止位。

因此,传送一个字节的字符需要 10 个 etu(etu 为时间单元),图示如下。



字符中的位边界发生于$(n-0.125)\sim(n+0.125)$etu,n 是起始位下降边之后的边沿数$(1\leqslant n\leqslant 9)$。

一个字符与下一个字符被额外保护时间(Extra Guard Time,EGT)分隔。

在相邻两个字符之间的 EGT，当字符从 PCD 发往 PICC 时是 0～57μs(0～6etu)，当字符从 PICC 发往 PCD 时是 0～19μs(0～2etu)。超出上述时间被理解为帧出错。

2）帧分界符

PCD 和 PICC 以帧的格式传送数据，每一帧由数据字符和帧 CRC(2B)组成。数据帧都以 SOF 标识符作为帧的开始，EOF 标识符作为帧的结束。

SOF 标识符的长度至少为 12etu，其组成如图 9.7(a)所示。

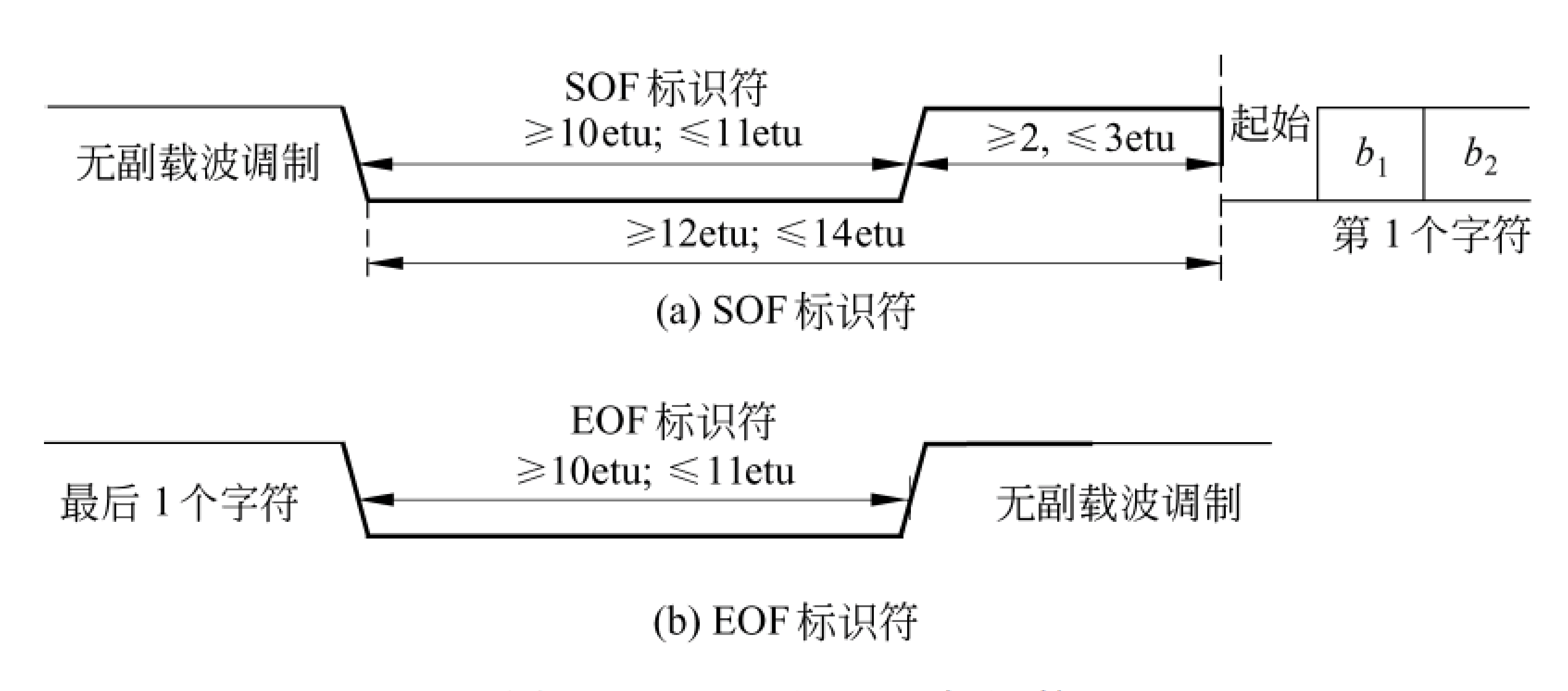


图 9.7　SOF 和 EOF 标识符

EOF 标识符的长度一般为 11etu，其组成如图 9.7(b)所示。

3）PICC 和 PCD 之间传送方向转换时的副载波和 SOF、EOF

从 PCD 发送转换到 PICC 发送的时序如图 9.8(a)所示。TR0(PCD EOF 和 PICC 产生副载波之间的时间)和 TR1(PICC 产生副载波到传送第 1 位之间的时间)可以在防冲突会话开始时定义(见 ATTRIB 命令)。

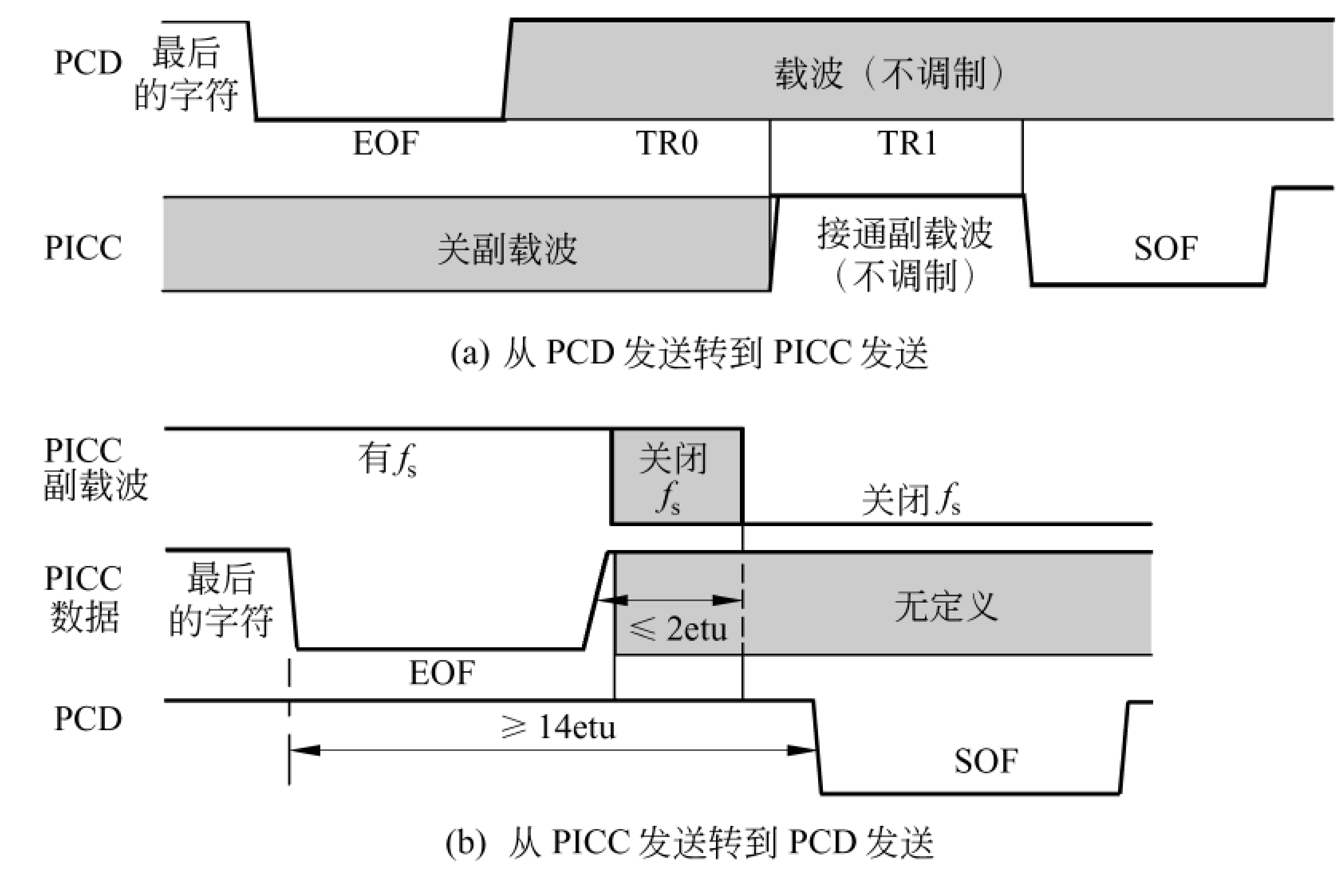


图 9.8　PICC 和 PCD 之间传送方向转换时的副载波和 EOF、SOF

从 PICC 发送转换到 PCD 发送的时序如图 9.8(b)所示。PICC 在发送 EOF 后将关闭副载波，关闭时间不迟于 EOF 结束后 2etu。PICC EOF 开始(下降边)和 PCD SOF 开始(下降边)之间的最小时间为 14etu。

当 PICC 打算开始发送信息时，才可接通副载波。

2. 数据帧

数据帧带有一个有效的 CRC-B 值。

数据帧：	Data 字节（n 字节）	CRC-B（2 字节）

3. 防冲突原理——时隙防冲突原理及举例

PCD 通过一组命令来管理防冲突过程。PCD 发出 REQB 命令启动多张 PICC 作出响应。如果有两张或更多卡同时响应，就发生了冲突。通过执行防冲突命令序列使得 PICC 完全置于 PCD 控制之下，在每一时刻只处理一张卡。

防冲突方案以时隙（time slot）为基础，时隙的个数由 REQB 命令中的参数决定，其范围为 1 至某个整数 N。假如有多张 PICC 进入 PCD 射频场，当接收到请求命令（REQB）时，每张卡各自产生一个随机时隙 $R(1\leqslant R\leqslant N)$，然后 PCD 发送时隙标记（slot-MARKER）命令，在命令中给出 R 值，该命令的功能是读取处于第 R 个时隙中的 PICC 标识码（卡的唯一序列号或其他）。当 N 的数值较小时，就有较大概率使两张（或以上）PICC 产生相同的 R，于是就有两张（或以上）的 PICC 送回标识码，这就是冲突。举例如下：如果 $N=3$，且有 5 张 PICC 进入 PCD 的有效射频场，假设在接收到 REQB 命令后，有两张卡产生的 $R=1$，两张卡的 $R=2$ 和 1 张卡的 $R=3$。然后 PCD 发出时隙标记命令（假设读取 $R=1$ 的 PICC 标识码），发现有冲突。再发时隙标记命令，顺序读出 $R=2$ 和 $R=3$ 的 PICC 标识码，终于得到无冲突的 $R=3$ 的 PICC 标识码。接着 PCD 与无冲突的 PICC 建立一个通信通道进行应用处理。处理完后 PCD 再重复发出 REQB 命令，已处理过的 PICC 不再接收此命令，因此仅有 4 张卡需要再处理，各自再次产生新的随机时隙 R，如果 N 仍等于 3，那么发生冲突的概率将减少。如此进行下去，直到所有的卡处理完毕。需要指出的是，当多次发送时隙标记命令时，命令中的 R 值可由 PCD 任意指定，不一定非得顺序增加。

上面提到的命令在后面命令集中介绍。

Type B 的命令集允许 PCD 执行不同的防冲突管理策略，这个策略由应用设计者制定。

4. PICC 状态描述

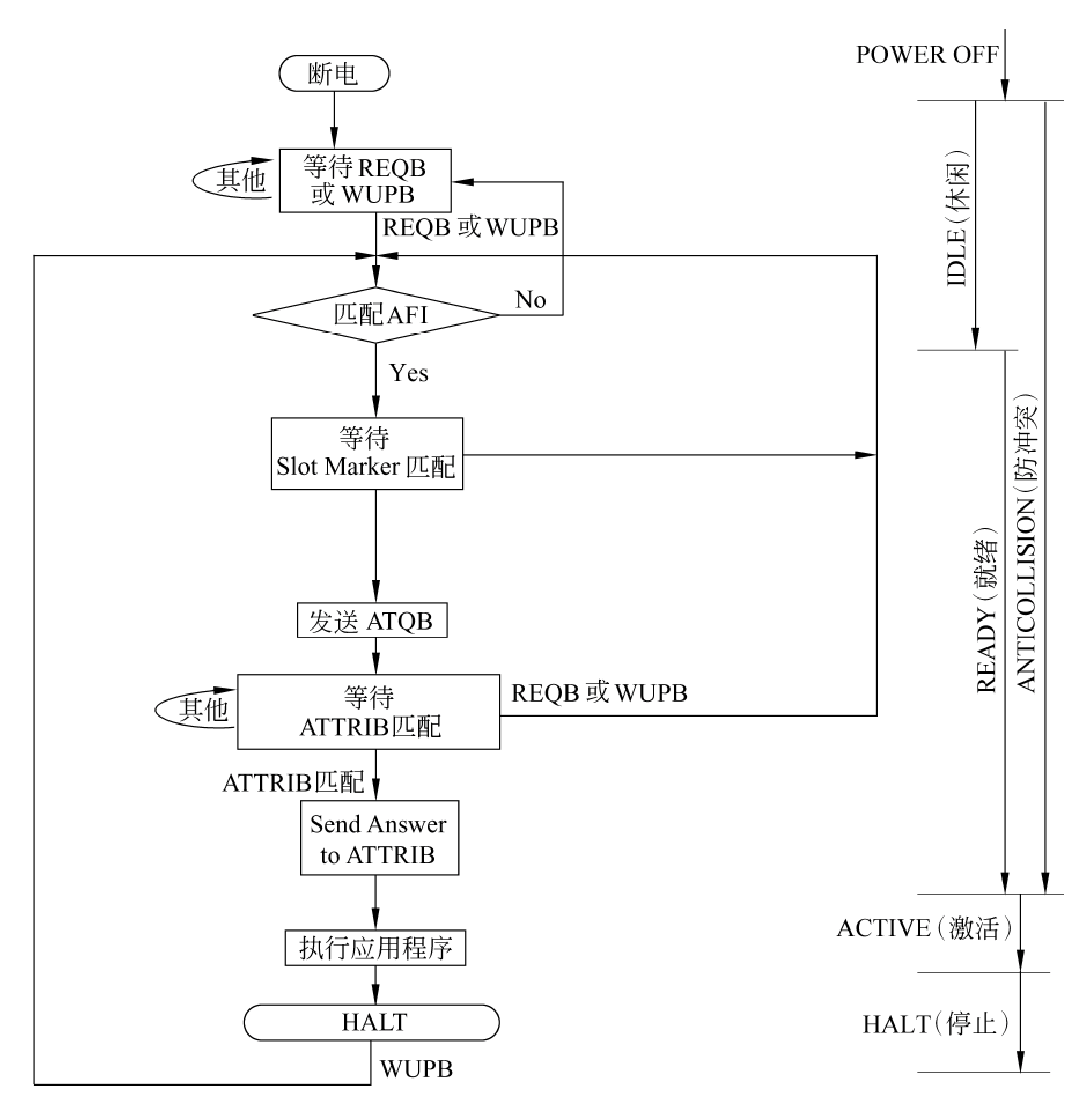
在防冲突序列中，PICC 的具体操作是根据 PCD 命令和 PICC 所处的状态及状态间的转换条件确定的。图 9.9 所示为 PICC 状态转换流程图。

有如下 6 种状态。

（1）断电（POWER OFF）状态。PICC 由于不在载波能量场内而处于断电状态。如果 PICC 处于一个能量足够大的激励磁场内（$H_{min}=1.5$A/m），则它将在不大于 5ms 的延时内进入 IDLE 状态。

（2）休闲（IDLE）状态。PICC 生成电压，监听 REQB 或 WUPB 命令帧，当接收到有效的 REQB 或 WUPB 帧（含有参数 N 和匹配的应用标识符）时，PICC 进入就绪（READY）状态。

（3）就绪（READY）状态。PICC 等待至收到一带有匹配时隙号 R 的 Slot-MARKER 命令，向 PCD 返回 ATQB。



注：AFI 为应用标识符。见 REQB/WUPB 命令

图 9.9　PICC 状态转换流程图(举例)

PCD 再发出 ATTRIB 命令。假如 ATTRIB 命令的 PUPI(见 ATTRIB 命令)与 PICC 中的 PUPI 匹配，PICC 就进入激活(ACTIVE)状态，否则仍保留在原状态。

(4) 激活(ACTIVE)状态。进入本状态后，PICC 监听更高层的报文(命令帧)，完成应用目标。

PICC 接收到 HALT 命令时，将进入 HALT 状态。

(5) HALT 状态。PICC 静止，不发出负载调制也不再参与防冲突循环。如果射频场消失，PICC 回到断电(POWER-OFF)状态。

5. 命令集

REQB/WUPB、Slot-MARKER、ATTRIB 和 HALT 命令都是由 PCD 发出的。

所有防冲突命令的前缀字节(APf)为×××××101。

PCD 发出的命令 REQB/WUPB 及 PICC 发出的响应 ATQB 如下。

1) REQB/WUPB 命令

处于 IDLE 和 READY 状态的 PICC 将处理该命令。WUPB 还用于唤醒 HALT 状态中的 PICC。

(1) REQB/WUPB 命令格式：

MSB　　　LSB	MSB　　　LSB	MSB　　　LSB	MSB　　　LSB
APf	AFI	PARAM	CRC_B
1B	1B	1B	2B

APf='05'=00000101。

- AFI(应用类型标识符)：代表由 PCD 指定的应用类型，AFI 的作用是在 ATQB 之前预选 PICC，只有那些具有 AFI 指定应用类型程序的 PICC 才能响应 REQB 命令。
- PARAM 编码：

RFU				REQB/ WUPB	M		
b_8	b_7	b_6	b_5	b_4	b_3	b_2	b_1

$b_4=0$ 为 REQB 命令，$b_4=1$ 为 WUPB 命令。

M 是防冲突的主要参数，时隙总数 $N=f(M)$。

$M(b_3\ b_2\ b_1)$	000	001	010	011	100	101	11×
N	$2^0=1$	$2^1=2$	$2^2=4$	$2^3=8$	$2^4=16$	RFU	RFU

对于每个 PICC，在第一个时隙内响应 ATQB 的概率为 $1/N$(即产生随机数 $R=1$ 的概率)。

(2) ATQB 响应。

ATQB 格式：

MSB	MSB　　　LSB	MSB　　　LSB	MSB　　　LSB	MSB　　　LSB
APa	Identifier(PUPI)	Application Data	Protocal Info	CRC_B
1B	4B	4B	2B	2B

- 前缀字节：APa='50'=01010000。
- 标识符(PUPI)：伪唯一的 PICC 标识符(Pseudo-Unique PICC Identifier，PUPI)用于区分 PICC，可以是唯一的 PICC 序列号；或 PICC 接收每一个 REQB 命令后计算而得的随机数等。PUPI 只有在 IDLE 状态下才能改变。
- 应用数据(Application Data)：该数据用来通知 PCD，在 PICC 上安装了哪些应用，这些数据允许在有多个 PICC 存在时，PCD 选择它所需的 PICC。
- 协议信息(Protocal Info)提供以下内容。

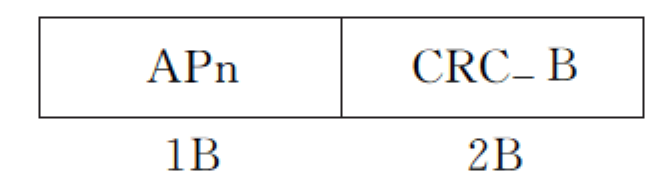
① 帧等待时间是 PCD 帧结束后到 PICC 响应的最大时间。

② PICC 支持的位速率为 106Kb/s、212Kb/s、424Kb/s 或 847Kb/s。

③ 帧长度为 16～256B。

2) Slot-MARKER 命令

命令格式：



APn	CRC_B
1B	2B

APn='×5'=nnnn0101，其中 nnnn 为时隙编号 R，为 1～15。在 REQB/WUPB 命令后，Slot-MARKER 命令来指定时隙 *R*，发送的时隙编号并不一定要按顺序增加。

PICC 对本命令的响应为 ATQB。

3）ATTRIB 命令

该命令包括选择一张 PICC 所需要的信息。

PICC 接收此命令，并被选择后(PUPI 匹配)，将与一个唯一的未用通道 CID 相联系，该 PICC 不再响应除包括唯一 CID 以外的任何命令。为再次响应一个新的 REQB 命令，PICC 应该先解除选中(或通过断电/通电过程复位)。

ATTRIB 命令格式：

APc	Identifier	参数	CRC_B
1B	4B	4B	2B

APc='1D'=0001 1101。

• Identifier(标识符)编码：标识码 PUPI 是 PICC 在 ATQB 响应中所发送的。

• 参数编码：包括 TR0、TR1、E0F、S0F 和位速率等。

① TR0 告诉 PICC，在 PCD 命令结束后到响应(发送副载波)之前的最小延迟时间。

② TR1 告诉 PICC，从副载波接通到数据开始发送之间的最小延迟时间。

③ EOF 和 SOF：b_4 或 b_3 指明 PCD 是否支持 EOF 或 SOF。若不需要，可以减少通信开销。

④ 可被 PCD 接收到的最大帧长度和位速率选择。

4）HALT 命令及响应

该命令将 PICC 置为 HALT 状态。在该状态 PICC 不响应 REQB 命令，仅对 WUPB 命令做出响应。

HALT 命令格式：

'50'	标识码	CRC_B(AID)
1B	4B	2B

9.4 ISO/IEC 15693-2 空中接口和初始化

本部分提出了在邻近式耦合设备(Vicinity Coupling Device，VCD)和邻近式卡之间提供能量和双向通信的规范。

能量传送到 VICC 是通过 VCD 和 VICC 中的耦合天线用射频 RF 来完成的，并通过射频的调制实现双向通信。RF 工作场的频率为 13.56MHz±7kHz。VICC 应在 150mA/m(最小有效值)～5A/m(最大有效值)的工作场内工作。

9.4.1 VCD 到 VICC 的通信信号接口

1. 调制

采用 ASK 的调制原理，进行 VCD 到 VICC 的通信。使用两个调制指数——10%～30%和 100%（调制指数＝$(a-b)/(a+b)$），波形与 ISO/IEC 14443 基本一致，如图 9.2 和图 9.3 所示。

2. 数据速率和数据编码

数据编码采用脉冲位置调制来实现。

VICC 支持两种数据编码方式（256 取 1 和 4 取 1）。

1）数据编码方式：256 取 1

一个字节的值（0～255）可以通过一个“间隙”的位置来表示。在 256 个连续时间内取 1 个间隙位置确定了该字节的值。一个间隙周期为 $256/f_c$（约 18.88μs）。因此，传输一个字节约 4.833ms（等于 256×18.88μs），所得到数据速率是 1.65 Kb/s（$f_c/8192$）。

图 9.10 所示为 256 取 1 编码方式。

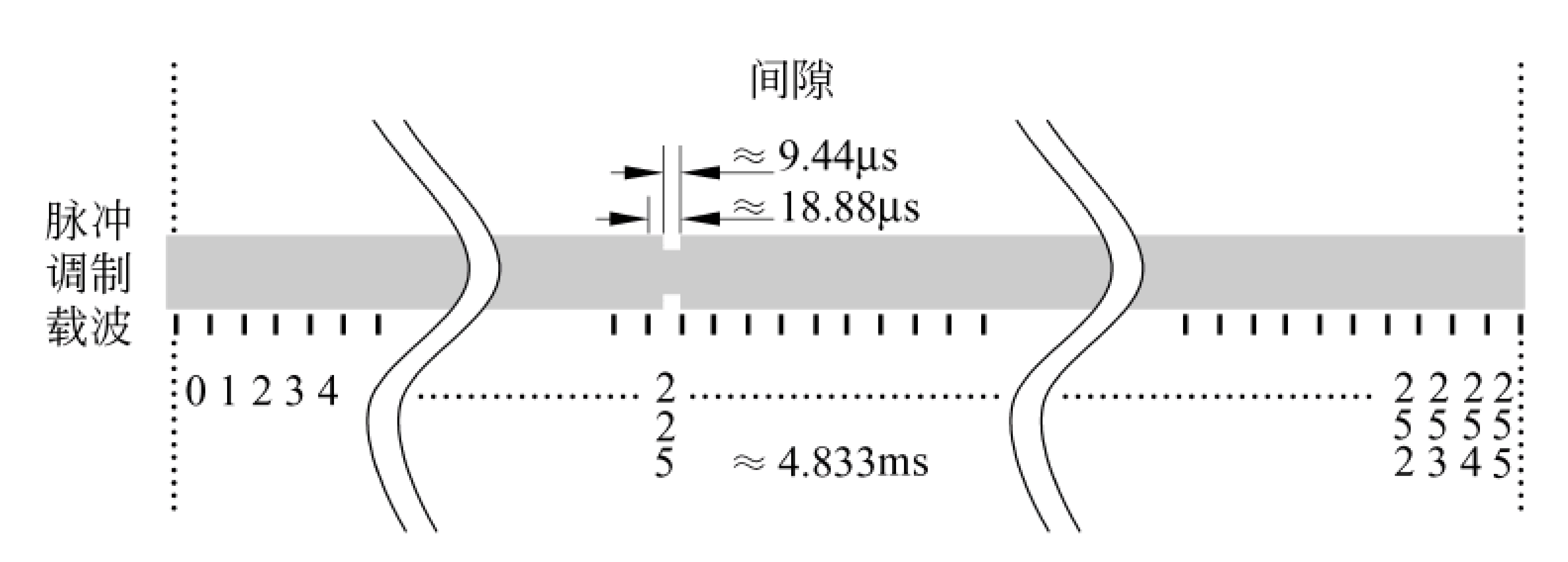


图 9.10　256 取 1 编码方式

在图 9.10 中，数据'E1'＝11100001_2＝225，是由 VCD 发送给 VICC 的。

间隙出现在确定该值的时间周期位置的后一半期间，如图 9.11 所示。

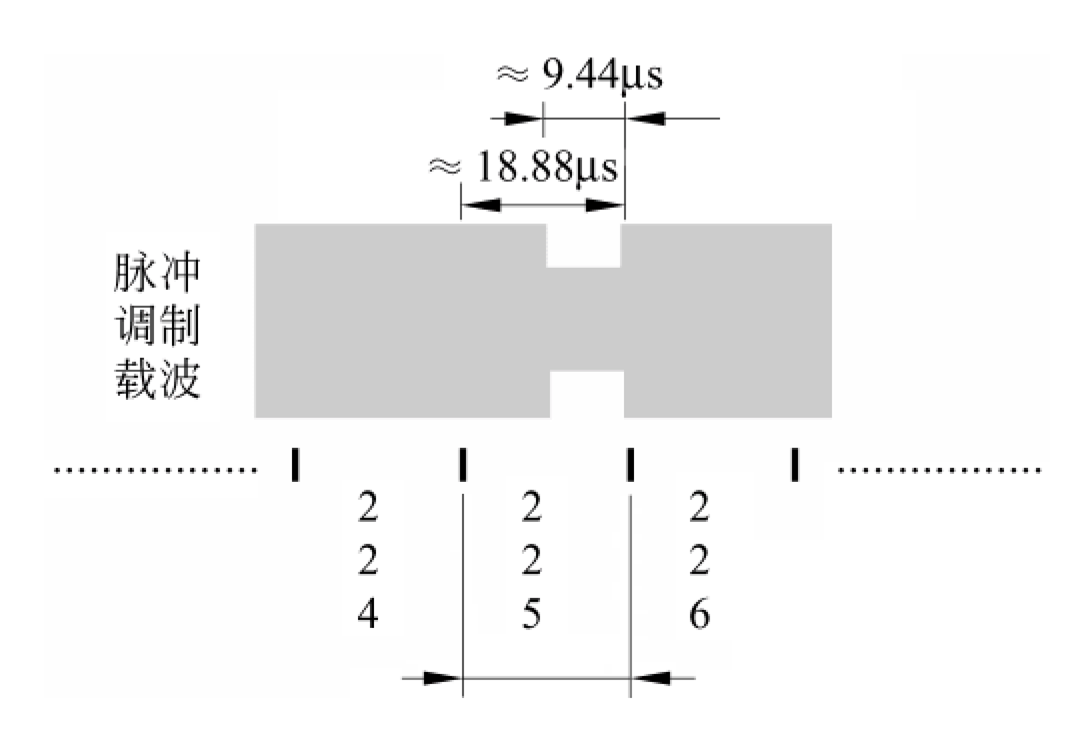


图 9.11　一个时间周期的细节

2）数据编码方式：4 取 1

通过 4 个间隙位置来确定两位数值$(00～11)_2$。4 个连续的“位对”构成 1 个字节，其中首先传送最低的有效“位对”。所得到的数据速率为 26.48Kb/s（$f_c/512$）。

图 9.12 所示为 4 取 1 脉冲位置和编码。

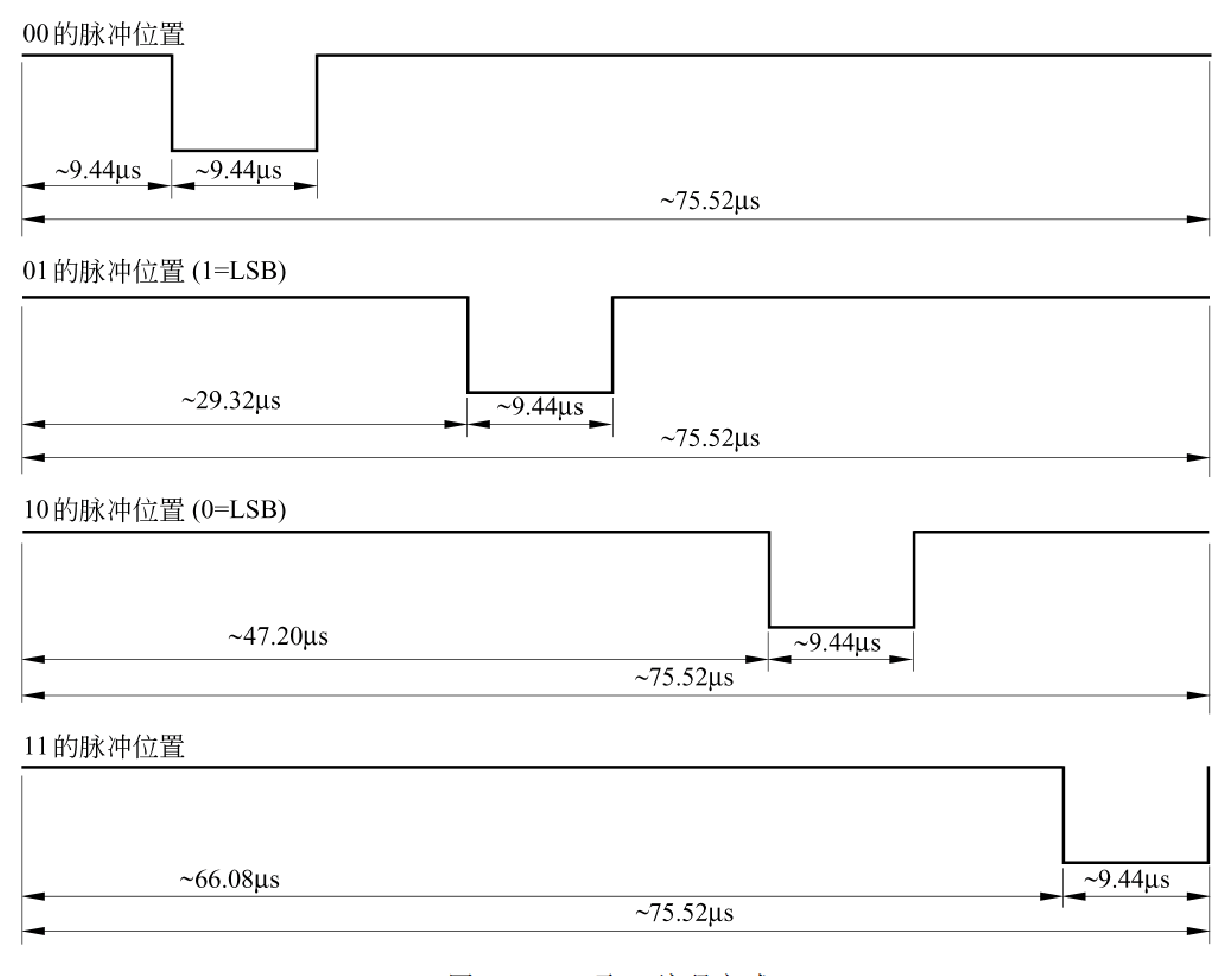


图 9.12　4 取 1 编码方式

例如，图 9.13 所示为 VCD 传输的'E1'＝11100001_2＝225_{10}。

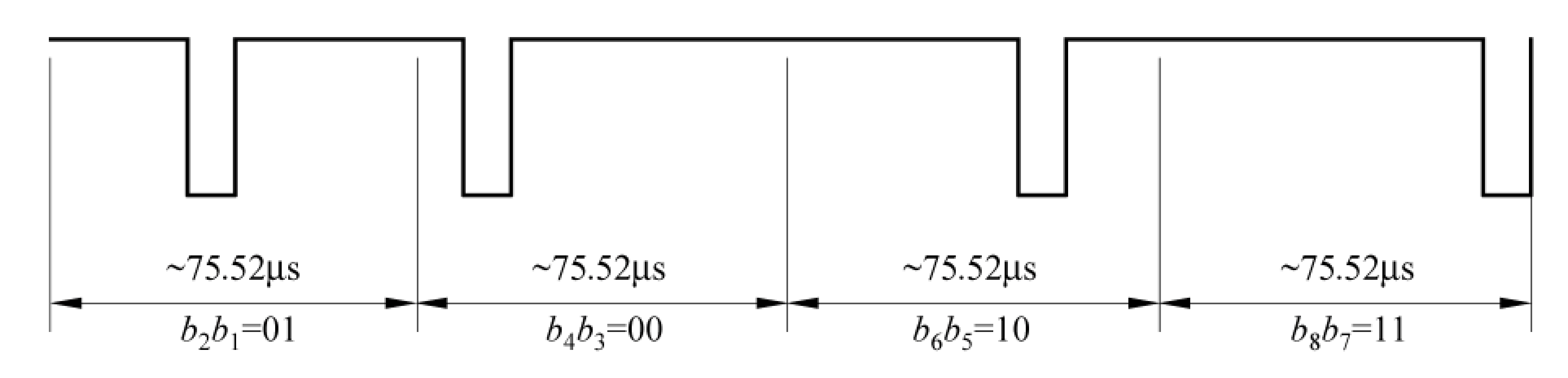


图 9.13　4 取 1 编码示例(11100001)

3. VCD 到 VICC 的帧

由帧开始(Start Of Frame，SOF)和帧结束(End Of Frame，EOF)来定界，并使用特定编码来实现。

VICC 应准备好在发送帧给 VCD 后的 300μs 内接收来自 VCD 的帧。

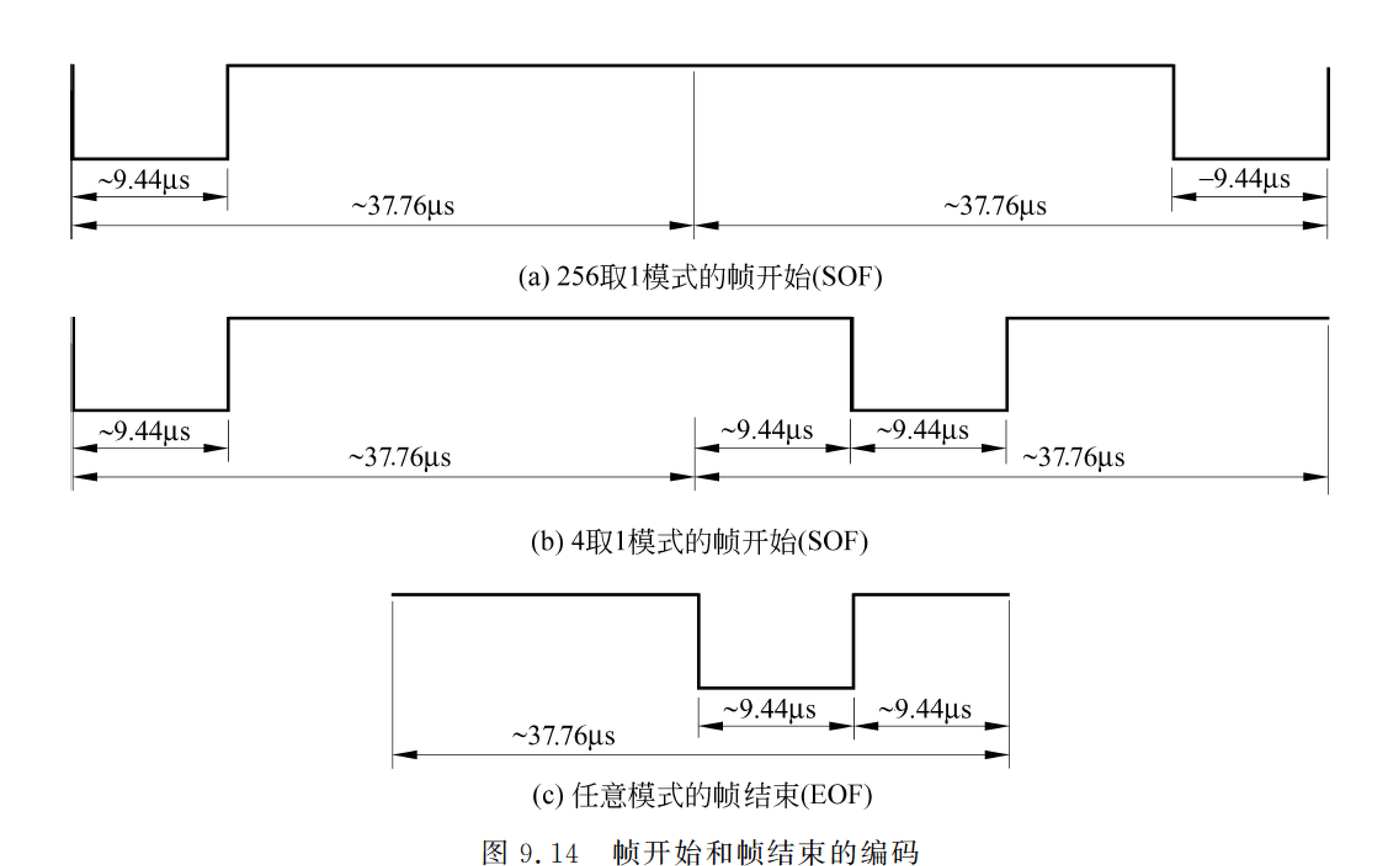
VICC 应准备好在能量场激活 1ms 内接收帧。

图 9.14 所示为 SOF 和 EOF 的编码。

9.4.2　VICC 到 VCD 的通信信号接口

1. 负载调制

VICC 借助电感耦合区域与 VCD 通信，VICC 通过 PCD 发送来的载波产生具有频率



(a) 256取1模式的帧开始(SOF)

(b) 4取1模式的帧开始(SOF)

(c) 任意模式的帧结束(EOF)

图 9.14 帧开始和帧结束的编码

f_s 的副载波,该副载波是通过切换 VICC 中的负载产生的。

负载调制幅度应至少为 10mV。

2. 副载波

VCD 使用一种或两种副载波,VICC 应支持两种方式。

当使用一种副载波时,副载波负载调制频率 f_{s1} 为 $f_c/32$(≈423.75kHz)。

当使用两种副载波时,频率 f_{s1} 为 $f_c/32$(≈423.75kHz),频率 f_{s2} 为 $f_c/28$(≈484.28kHz)。

若存在两种副载波,它们之间应有连续的相位关系。

3. 数据传送速率

可以使用低或高数据速率。VICC 应支持表 9.5 所示的数据速率。

表 9.5 数据速率

数据速率	单 副 载 波	双 副 载 波
低	6.62Kb(f_c/2048)	6.67Kb(f_c/2032)
高	26.48Kb(f_c/512)	26.69Kb(f_c/508)

4. 位和编码

数据使用曼彻斯特编码。下面的讨论涉及 VICC 到 VCD 的高数据速率。对低数据速率,如果使用同样的副载波频率,脉冲数和时间应乘以 4。

1) 使用单副载波时的位编码

逻辑 0 以 $f_c/32$(≈423.75kHz)的 8 个脉冲开始,接着是未调制的时间 $256/f_c$(≈18.88μs),如图 9.15 所示。

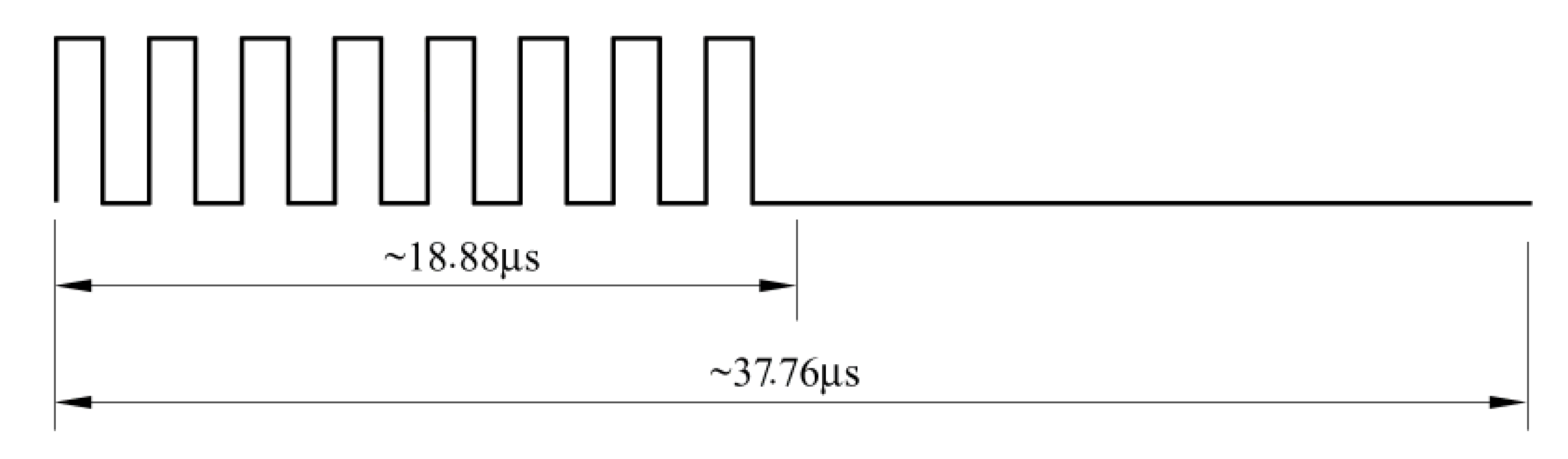


图 9.15　逻辑 0(单副载波)

逻辑 1 以未调制的时间 $256/f_c$(≈ 18.88μs)开始,接着是 $f_c/32$(≈ 423.75kHz)的 8 个脉冲,如图 9.16 所示。

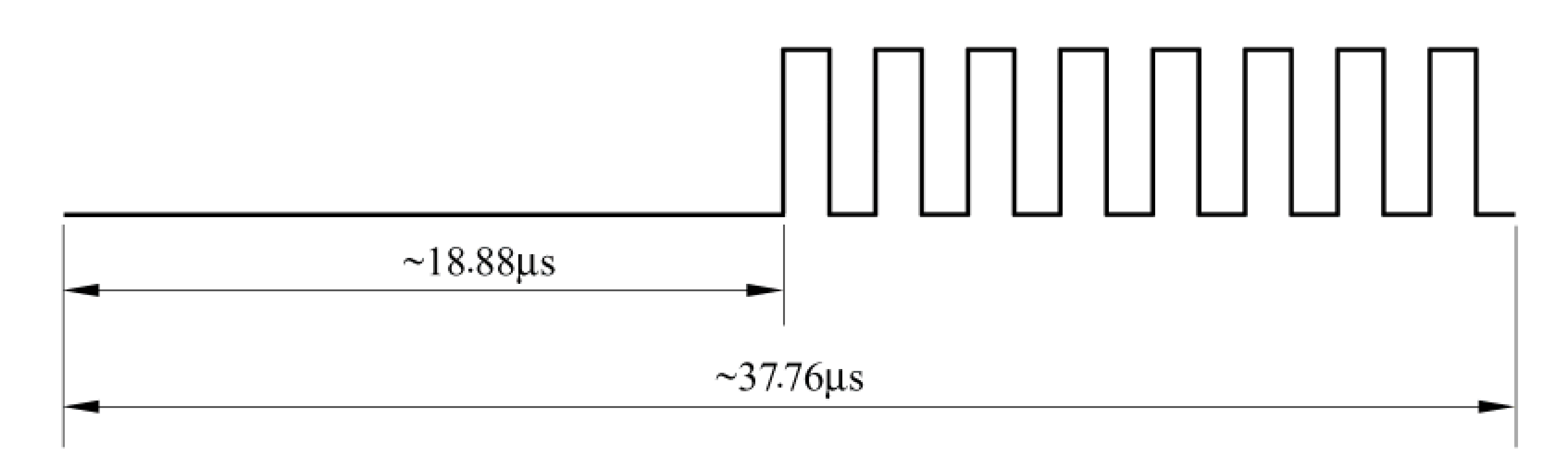


图 9.16　逻辑 1(单副载波)

2) 使用两种副载波时的位编码

逻辑 0 以 $f_c/32$(≈ 423.75kHz)的 8 个脉冲开始,接着是 $f_c/28$(≈ 484.28kHz)的 9 个脉冲,如图 9.17 所示。

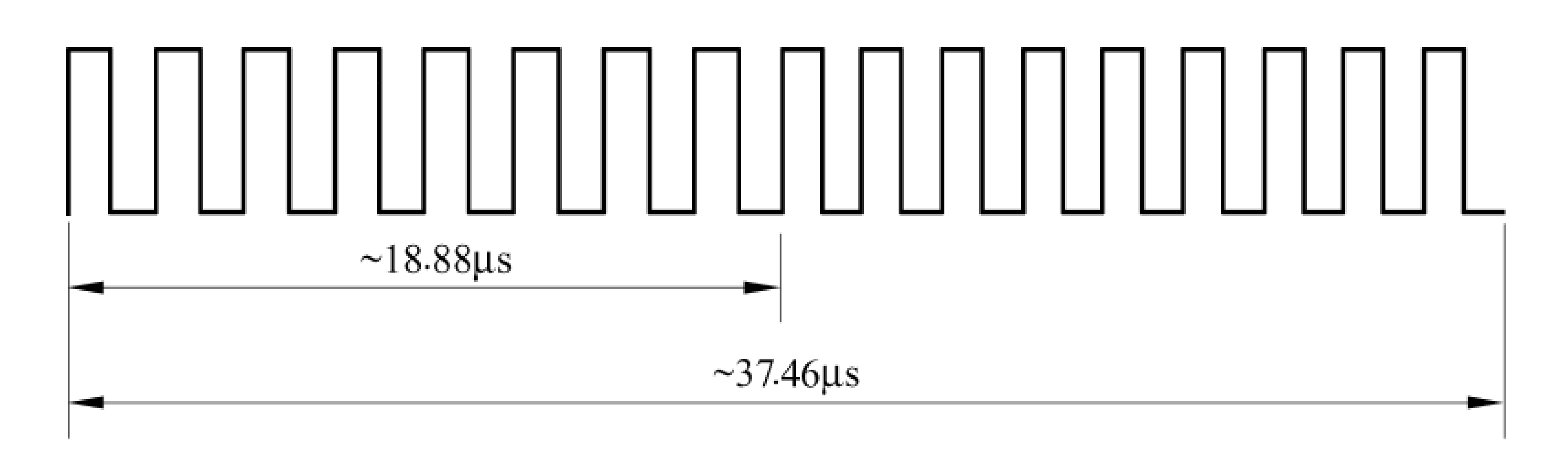


图 9.17　逻辑 0(两种副载波)

逻辑 1 以 $f_c/28$(≈ 484.28kHz)的 9 个脉冲开始,接着是 $f_c/32$(≈ 423.75kHz)的 8 个脉冲,如图 9.18 所示。

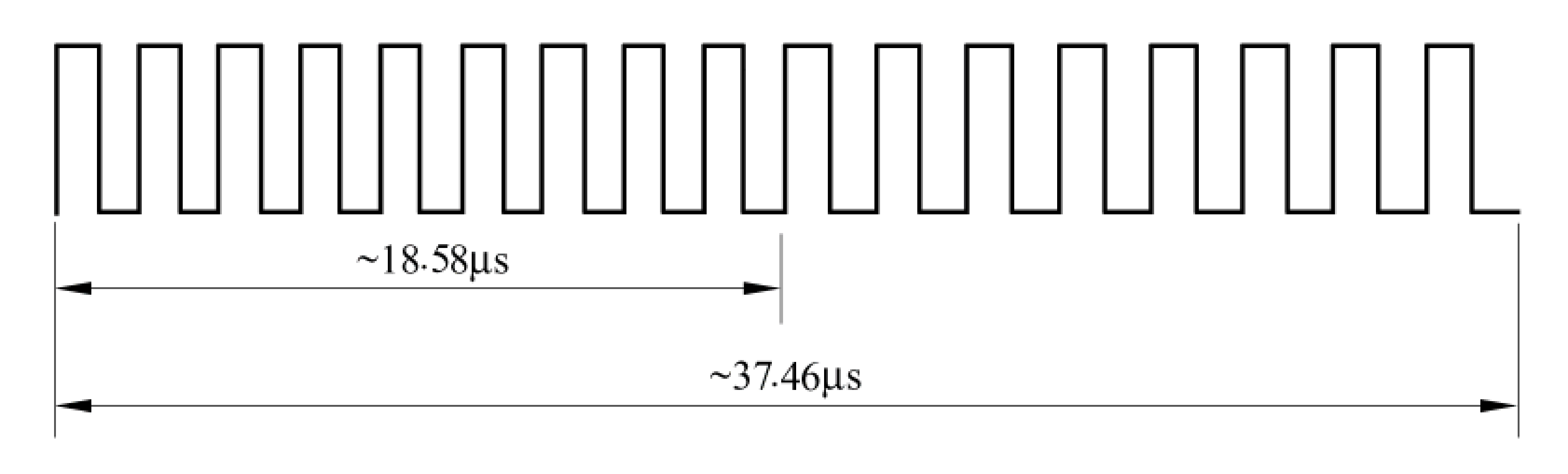


图 9.18　逻辑 1(两种副载波)

5. VICC 到 VCD 的帧

下面所有定时涉及 VICC 到 VCD 的高数据速率。

对低数据速率，如果使用同样的副载波频率，脉冲数和时间应乘以 4。

VICC 应准备好在发送帧给 VCD 后的 300μs 内接收来自 VCD 的帧数据。

1) 使用单副载波时的 SOF(图(9.19(a))

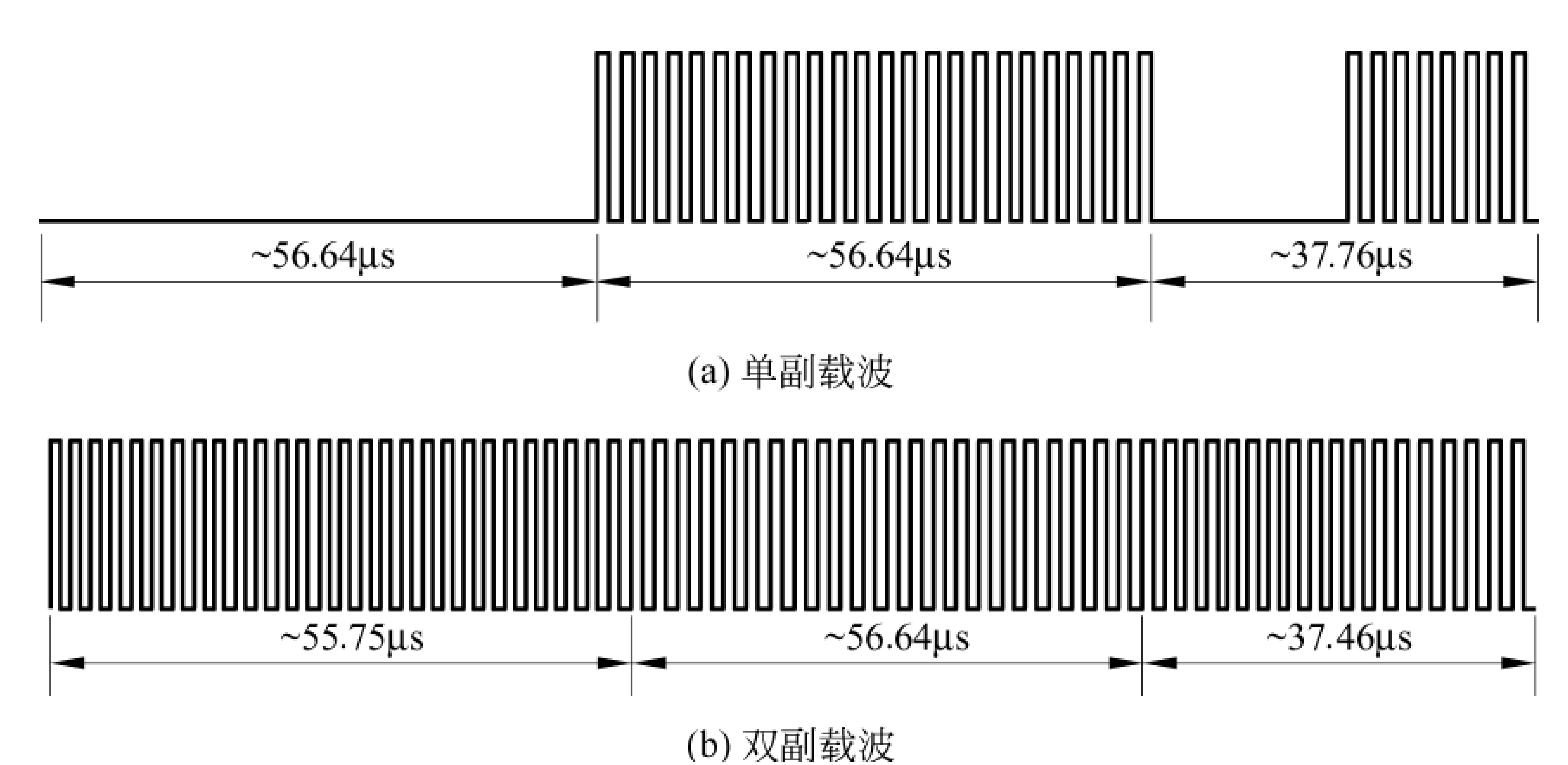


图 9.19　使用单副载波或双副载波的 SOF

SOF 包含如下 3 个部分。

(1) 未调制时间 768/f_c(≈56.64μs)。

(2) f_c/32 (≈423.75kHz)的 24 个脉冲。

(3) 逻辑 1，它以未调制时间 256/f_c(≈18.88μs)开始，接着是 f_c/32(≈423.75kHz)的 8 个脉冲。

2) 使用双副载波时的 SOF(图 9.19(b))

SOF 包含如下 3 个部分。

(1) f_c/28(≈484.28kHz)的 27 个脉冲。

(2) f_c/32(≈423.75kHz)的 24 个脉冲。

(3) 逻辑 1，它以频率为 f_c/28(≈ 484.28kHz)的 9 个脉冲开始，接着是 f_c/32(≈423.75kHz)的 8 个脉冲。

3) 使用单副载波时的 EOF(图 9.20(a))

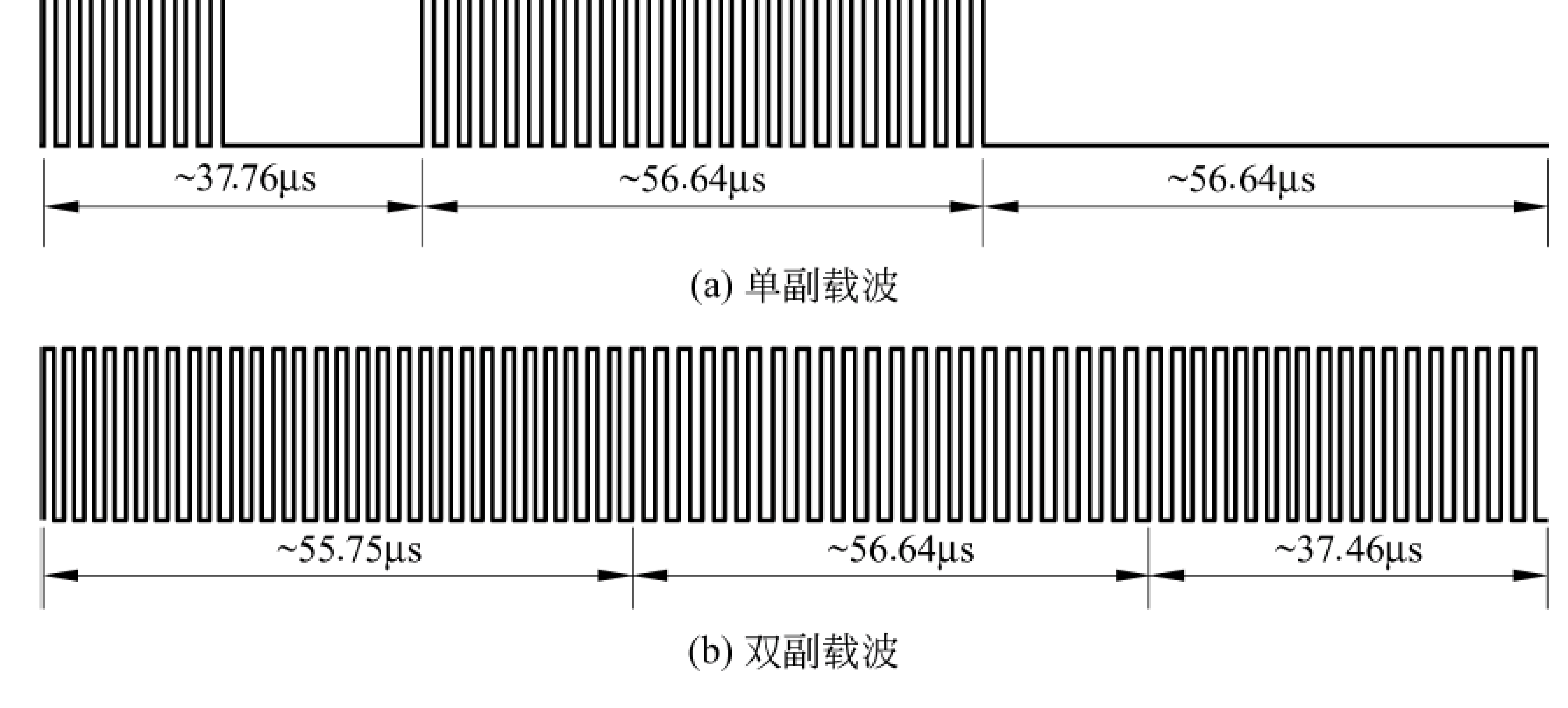


图 9.20　使用单副载波或双副载波的 EOF

EOF 包含如下 3 个部分。

(1) 逻辑 0,它以 $f_c/32$(≈423.75kHz)的 8 个脉冲开始,接着是未调制时间 $256/f_c$(≈18.88μs)。

(2) $f_c/32$(≈423.75kHz)的 24 个脉冲。

(3) 非调制时间 $768/f_c$(≈56.64μs)。

4) 使用双副载波时的 EOF(图 9.20(b))

EOF 包含如下 3 个部分。

(1) 逻辑 0,它以 $f_c/32$(≈423.75kHz)的 8 个脉冲开始,接着是 $f_c/28$(≈484.28kHz)的 9 个脉冲。

(2) $f_c/32$(≈423.75kHz)的 24 个脉冲。

(3) $f_c/28$(≈484.28kHz)的 27 个脉冲。

9.5 ISO/IEC 15693-3 防冲突和传输协议

当有多张 VICC 卡处于 PCD 的工作场内,就有可能发生冲突。本协议采用的防冲突方法是由 VCD 发出清点命令,在 VICC 配合下,最终清点出场内所有 VICC 的唯一标识码 UID。

传输协议定义了 VCD 和 VICC 之间的命令和双向交换的机制。命令都是由 VCD 发出的,VICC 对每一个命令作出响应。每一次命令和每一次响应都各自包含在一帧内,帧分隔符为 SOF、EOF,一帧中传输的位的个数是 8 的倍数,即整数个字节。在通信中,单字节首先传输最低有效位;多字节首先传输最低有效字节,每字节最先传输最低有效位。

9.5.1 命令和响应的通用格式、VICC 状态及其转换

1. 命令通用格式

SOF	标志	命令代码	参数	数据	CRC	EOF

标志、命令代码、CRC(校验码)、SOF 和 EOF 字段是必备的,参数和数据字段是可选的(由各个命令决定)。

命令的标志字段说明了 VICC 完成的动作(采用单副载波或双副载波、高或低数据传输率、防冲突的时隙 1 或 16)及相应的可选字段(UID 和 AFI)是否存在。

2. 响应通用格式

SOF	标志	参数	数据	CRC	EOF

标志、CRC、SOF 和 EOF 字段是必备的,参数和数据字段则是可选的,由各个命令及其执行情况决定。

响应标志指示 VICC 的动作是否完成(有或无差错)。如果检测到差错,差错代码在

参数字段。

3. 响应格式的 3 种表示

(1) 当命令要求 VICC 返回数据，且执行无误时，以响应通用格式表示，其中参数和数据字段的内容随命令而定。

(2) 当命令不要求返回数据，且执行无错误时，其响应格式如图 9.21 所示。

(3) 无论命令是否要求返回数据，当执行有错误时，其响应格式如图 9.22 所示。

SOF	标志	CRC16	EOF

图 9.21 命令不要求返回数据且执行无错的响应格式

SOF	标志	差错代码	CRC16	EOF

图 9.22 命令执行有错时的响应格式

在其后描述命令和响应时，对第(2)种和第(3)种响应格式予以默认，不再重复介绍。

9.5.2 防冲突

防冲突系列(操作流程的处理)的目的，是清点出 VICC，清点的结果是得出 VCD 工作场中多个 VICC 唯一标识码 UID。VCD 通过发出清点命令启动它与卡之间的通信。

防冲突方案以时隙为基础，其工作原理参考 9.3.3 节(Type B 的防冲突)。

1. 清点命令和响应格式

VCD 在发出清点命令时，在标志字段中将时隙数目设置为期望值(1 个时隙或 16 个时隙)，然后在命令字段的后面加入掩码长度和掩码值(命令通用格式中的参数字段和数据字段)。清点命令格式如下(命令代码＝'01')。

SOF	标志	清点(命令)	掩码长度	掩码值	CRC16	EOF
	8位	8位	8位	0~64位	16位	

掩码长度指出掩码值的位数。掩码值是 VCD 欲清点的 VICC 的 UID(低位部分)，很可能不存在。

如果清点命令中的 AFI 标志已设置，则在清点命令中将增加 AFI 字段，此命令的格式如下。

SOF	标志	清点	可选的 AFI	掩码长度	掩码值	CRC16	EOF
	8位	8位	8位	8位	0~64位	16位	

AFI(应用标识符)表示由 VCD 标定的应用类型，只有支持该 AFI 应用类型的 VICC 才能从所有存在于 VCD 工作场的 VICC 中被挑选出来。

清点命令的响应格式如下。

SOF	标志	DSFID	UID	CRC16	EOF
	8位	8位	64位	16位	

响应中包括 DSFID 和 UID。DSFID(数据存储格式标识符)指出了数据在 VICC 存储器中是如何构成的。如果 VICC 不支持 DSFID 编码，将以'00'作为响应。UID 由 64 位

组成，由 IC 制造商写入到卡中。UID 格式如下。

MSB		LSB
64　　57	56　　49	48　　1
'E0'	IC 制造商代码	IC 制造商序列号

如果 VICC 检测到错误，发送响应如图 9.22 所示。

2. 防冲突操作流程举例

如果时隙数量是 16，那么在 VICC 中有 4 位时隙计数器，在开始执行“清点命令”时，将它清 0，假设有 5 个 VICC 在 VCD 工作场内的情况下，总结了可能发生的主要情况。操作步骤如下。

(1) VCD 发送由 EOF 终止的以帧表示的清点命令，时隙的数量为 16。各 VICC 随机产生各自的时隙编号。假设 VICC1 的时隙编号为 0，VICC(2 和 3)为 1，VICC(4 和 5)为 3，VICC 在执行清点命令过程中，时隙编号不变。

(2) VICC1 在时隙 0 发送其响应。VICC1 是发送响应的唯一 VICC，因此不会出现冲突，VCD 接收它的 UID 并为其注册。

(3) VCD 发送一个 EOF，意指切换到下一个时隙，即时隙计数器加 1，时隙计数值为 1。

(4) 在时隙 1 内，两个 VICC(2 和 3)发送它们的响应，产生冲突。VCD 检测到冲突，并且记住在时隙 1 发生冲突。

(5) VCD 发送一个 EOF，意指切换至下一个时隙(+1)，即时隙计数值为 2。

(6) 在时隙 2 内，没有 VICC 发送响应。因此，VCD 未检测到 VICC SOF，于是通过发送一个 EOF 来切换到下一个时隙(+1)，即时隙计数值为 3。

(7) 在时隙 3 内，来自 VICC(4 和 5)的响应引起另一冲突。

(8) 在时隙 4 到时隙 15，都没有 VICC 发生响应。

(9) VCD 决定发送一个寻址的命令(如一个读块)给 VICC1，其 UID 已被正确接收。

(10) 所有的 VICC 检测到 SOF，将退出防冲突序列。因为该命令是对 VICC1 寻址的，只有 VICC1 完成应用程序，发送其响应。

(11) 所有 VICC(除了已注册的 VICC)都就绪接收另一个命令。如果它是一个清点命令，时隙计数器重新从 0 开始。各 VICC 随机产生各自的时隙编号，即返回到步骤(1)。

注：VCD 还可以先循环发送清点命令，将 5 个 VICC 卡进行注册。然后发送读块(或其他)命令给 VICC1……直到所有 VICC 处理完毕。

3. 设想：1 时隙防冲突流程举例

设计一条命令，使所有在工作场中的 VICC 随机响应，返回 UID。VCD 将接收、检测所有未发生冲突的响应。当少量的 VICC 在工作场内时，该方法效果较好。

图 9.23 所示为 3 个 VICC 在工作场中的情况。

(1) VCD 发出一条命令，所有 VICC 响应，冲突发生。

(2) 然后 VICC1 和 VICC3 经过不同的持续时间后响应，导致冲突发生。

(3) VICC2 的单独响应被检测到。

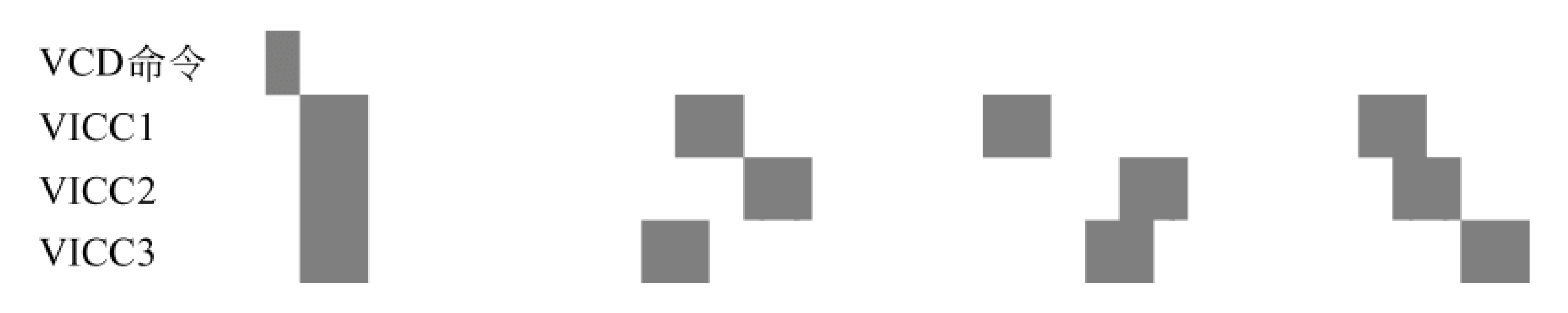


图 9.23　1 时隙多 VICC 读协议的 VICC 响应实例

(4) 然后 VICC1 的单独响应被检测到。

(5) VICC2 和 VICC3 的响应导致冲突发生。

(6) VICC1 和 VICC2 的响应导致冲突发生。

(7) 最后 VICC3 的响应被检测到。

各个 VICC 的响应时间间隔是由 VICC 自己决定的，可以随机生成，但相互之间不能相同。

9.5.3　命令和响应

本协议定义了 4 种类型命令：强制的、可选的、定制的和专有的。定制的和专有的由 IC 制造商设定。下面介绍清点命令(强制的)和读/写命令(可选的)。

执行本部分规定的命令前，已将 VICC 的存储器划分成固定容量的块，最多有 256 个块可被寻址，块的大小最多为 256 位，最大存储容量可达 8KB。

1. 清点命令

命令代码＝'01'。

当接收清点命令时，VICC 应执行防冲突序列。命令格式及响应格式已在前面描述。在指定时隙中，仅当 UID 的低位部分与命令中的掩码值相等的卡才能响应，因而可降低冲突概率。

2. 读单个块命令

命令代码 ＝'20'，命令格式如下。

SOF	标志	读单个块	[UID]	块编号	CRC16	EOF
	8位	8位	64位	8位	16位	

响应格式(无错误时)如下。

SOF	标志	[块安全状态]	数据	CRC16	EOF
	8位	8位	1块	16位	

注：[ ]内的项目是可选的(下同)。

当接收读单个块命令时，VICC 应读命令的块，并且在响应中发送它的数据值。

由命令中标志确定 VICC 是否返回块安全状态，接着是逐块顺序的块值。

3. 写单个块命令

命令代码 ＝'21'，命令格式如下。

SOF	标志	写单个块	[UID]	块编号	数据	CRC16	EOF
	8位	8位	64位	8位	1块	16位	

当接收写单个块命令时，将命令中包含的数据块写入 VICC，并且在响应中报告操作是否成功。

4. 读多个块命令

命令代码＝'23'，命令格式如下。

SOF	标志	读多个块	[UID]	第 1 个块编号	块数量	CRC16	EOF
	8位	8位	64位	8位	8位	16位	

响应格式如下。

<table>
<tr><td>SOF</td><td>标志</td><td>[块安全状态]</td><td>数据</td><td>CRC16</td><td>EOF</td></tr>
<tr><td></td><td>8位</td><td>8位</td><td>多块</td><td>16位</td><td></td></tr>
<tr><td></td><td></td><td colspan="2">当需要时，重复</td><td></td><td></td></tr>
</table>

执行读多个块命令时，VICC 应读命令块，并且在响应中返回它们的值。

由命令中标志确定 VICC 是否返回块安全状态，接着是逐块顺序的块值。

习题

1. 在 ISO/IEC 14443 国际标准中 Type A 和 Type B 两种非接触式卡在传递信息方面有什么区别？
2. 什么是冲突？Type A 和 Type B 的 IC 卡怎样实现防冲突？有什么差异？请说出防冲突的操作流程。
3. 为了实现非接触式 IC 卡的初始化和防冲突，在国际标准中定义了哪些命令？
4. 请叙述在 ISO/IEC 14443 中的 REQA、ATQA、REQB、ATQB 的作用及信息格式。
5. 接触式 IC 卡的国际标准 ISO/IEC 7816 与非接触式 IC 卡完全没有关系，这种说法对吗？
6. 请写出名词“时隙”“间隙”“API”“UID”“PUPI”“伪随机数”的含义。
7. 你认为依照 ISO/IEC 14443 中确定的命令是否满足设计 VICC 卡的需求？
8. ISO/IEC 7816 与 ISO/IEC 14443 中的指令格式表示方法是否相同？你认为造成这种情况的原因是什么？
9. VICC 可工作于一种或两种副载波频率下，这是用什么方法区别逻辑 0 和逻辑 1 的？
10. 叙述 VICC 防冲突原理。(1 时隙和多时隙)防冲突操作有什么基本差异？
11. 当有较多卡出现在 VCD 的工作场中时，应采用哪种防冲突协议(1 时隙或多时隙协议)？

第 10 章　RFID 标签空中接口标准 ISO/IEC 18000 系列

10.1　概述

RFID 标签和读写器之间通过相应的空中接口协议进行相互通信。空中接口协议定义了读写器与标签之间进行命令和数据双向交换的机制，即读写器发给标签的命令和标签发给读写器的响应。

目前，RFID 的空中接口标准中最受瞩目的是 ISO/IEC 18000 系列标准，适用于射频识别技术在物品管理中的应用。它涵盖了125kHz～2.45GHz 的通信频率，识读距离由几厘米到几十米，其中主要是无源标签，但也有些用于集装箱的有源标签。

ISO/IEC 18000-1 定义了在所有 ISO/IEC 18000 系列标准中空中接口定义所要用到的参数。还列出了所有相关的技术参数及各种通信模式，如工作频率、跳频速率、跳频序列、调制载波频率、占用频道带宽、最大发射功率、杂散发射、调制方式、调制指数、数据编码、位速率、标签唯一标识符、读处理时间、写处理时间、错误检测、存储容量、防冲突类型和标签识读数目等，为后续的各部分标准设定了一个框架和规则。

ISO/IEC 18000 的其他部分分别定义了在各种通信频率下的空中接口通信协议。

目前在 HF 频段的 13.56MHz 和 UHF 频段的 RFID 技术应用最为广泛。在 UHF 频段中，860～960MHz 频段一般用于无源标签，433MHz 一般用于有源标签。标签和读写设备之间的工作原理，在 HF 和 UHF 频段下是截然不同的，前者采用近距离磁场耦合的方式来工作，标签感应读写设备所产生的磁场信号，并依靠磁场的变化来传递信息，工作距离较近；后者采用反向散射的方式来工作，标签利用接收到的由读写器发出的射频能量，将编码信息利用电波传播回去，其工作距离较远。

10.2　空中接口标准化参数

ISO/IEC 18000-1 定义了两组空中接口数据链路参数：从读写器到 RFID 标签（在本章中简称“标签”）的参数（以符号 Int 表示），从标签到读写器的参数（以符号 Tag 表示）。此处说明每个参数的含义，具体指标将在ISO/IEC 18000系列标准的其他部分用表格方式描述。

1. 工作频率范围（Int：1，Tag：1）

规定通信链路工作的频率范围。

（1）默认工作频率（Int：1a，Tag：1a）。规定读写器和标签建立通信的工作频率。所给值是已调制信号的中心频率或范围。

（2）工作信道（适用于扩频系统，Int：1b，Tag：1b）。规定读写器至标签链路（或反向）

工作频率的数量和数值。所提供的数值是已调制信号的中心频率。

(3) 工作频率精度(Int:1c,Tag:1c)。用 ppm 指出载波频率和指定标称频率之间的最大偏差,1ppm 为百万分之一,如 2450MHz 载波的百万分之一允许载波频率范围为 2450MHz±2.45kHz。

(4) 跳频速率(适用于跳频[FHSS]系统,Int:1d,Tag:1d)。规定 FHSS(Frequency Hopping Spread Spectrum)中心频率驻留时间的倒数。

(5) 跳频序列(适用于跳频[FHSS]系统,Int:1e,Tag:1e)。规定 FHSS 发射机选择一个 FHSS 频道的跳频频率的伪随机序列列表。

2. 占用信道带宽(Int:2,Tag:2)

规定占用一个特定信道的通信信号的带宽。

最小接收机带宽(Int:2a,Tag:2a)规定接收机所能够接收到的所有频率或单个频率的最小频率范围。

3. 发送最大 EIRP(Int:3,Tag:3)

规定由读写器(或标签)天线发送的最大有效全向辐射功率 EIRP(Effective Isotropic Radiated Power)。

4. 杂散发射(Int:4,Tag:4)

无用的频率输出定义为杂散发射,包括谐波、子谐波、本机振荡和其他寄生发射。

5. 发射频谱掩码(Int:5,Tag:5)

规定读写器(或标签)发射的作为频率函数的最大功率或场强。

6. 定时(Int:6,Tag:6)

(1) 发送-接收转换时间(Int:6a,Tag: 6a):规定从标签发送完对读写器的答复到准备好接收下一个读写器询问的最长时间。

(2) 接收-发送转换时间(Int:6b,Tag: 6b):规定标签接收完一个读写器询问到标签开始回复询问的最长时间。

(3) 读写器发送功率上升时间(Int:6c):规定读写器发送功率从稳态输出功率水平的 10%上升到 90%所需的最长时间。

(4) 读写器发送功率下降时间(Int:6d):规定读写器发送功率从稳态输出功率水平的 90%下降到 10%所需的最长时间。

7. 调制(Int:7,Tag:7)

规定编码数据对载波的键控方式。应描述成与一般理解意义上的方法相一致,如幅移键控、相移键控、频移键控、线性调幅和调频。

(1) 扩频序列(适用于直接序列[DSSS]系统)(Int:7a,Tag: 7a)。规定对每一个逻辑数据位编码的码片(Chip)序列。

(2) 码片速率(适用于扩频系统,Int:7b,Tag: 7b)。规定扩频序列调制载波的频率。

(3) 码片速率精度(适用于扩频系统,Int:7c,Tag:7c)。规定码片速率的允许误差,用 ppm 表示。

(4) 调制指数(Int:7d) 。规定调制指数为$[a-b]/[a+b]$,a 和 b 分别为信号振幅的峰值和最小值。调制指数通常用百分比表示。

(5) 开关比率(Tag:7d)。适用于 ASK 调制(包括 OOK),ASK 调制信号的峰值振幅和最小振幅的比率。

(6) 副载波频率(Tag: 7e)。用于调制载波频率的频率,副载波由数据信息或编码调制。

(7) 副载波频率精度(Tag:7f)。任何原因引起的副载波频率的最大误差。通常情况下,用%表示或以副载波频率的 ppm 表示。

(8) 副载波调制(Tag:7g)。用编码数据完成的副载波键控,与通常描述的方法是一致的,如幅移键控、相移键控、频移键控、线性调幅和调频。

(9) 占空比(适用于 OOK 调制,Int:7h,Tag:7h)。定义为从有信号时间与整个通信持续时间的比率。

(10) 调频偏移(适用于调频,Int:7i,Tag:7i)。规定调制波的最大瞬时频率和载波频率的差值。

(11) 调制脉冲上升和下降时间(Int:7j)。定义调制脉冲上升和下降时间。

8. 数据编码(Int:8,Tag:8)

规定基带信号的表示方式,如双相编码(曼彻斯特、FM0、FM1、差分曼彻斯特)、NRZ 和 NRZI。

9. 位速率(Int:9,Tag:9)

规定每秒传输的位数,以位/秒来表示。

位速率准确度(Int:9a,Tag: 9a):规定位速率与标称值间的最大偏离程度,以 ppm 表示。

10. 发送调制准确度(Int:10,Tag:10)

规定在码片发送时段测量得到的峰值矢量误差级。

11. 前同步码(Int:11,Tag:11)

在数据前设置的同步码,可以是未调制载波或已调制载波,这取决于编码后的信道要求。

(1) 前同步码长度(Int:11a,Tag: 11a)。规定以位表示的前同步码的长度。

(2) 前同步码波形(Int:11b,Tag: 11b)。规定前同步码在信道上的信号形状。

(3) 位同步序列(Int:11c,Tag:11c)。接收机利用该序列与输入位流保持同步。

(4) 帧同步序列(Int:11d,Tag:11d)。用于指示一个数据帧开始的位序列。

12. 不规则性(适用于扩频系统,Int:12,Tag:12)

发送的所有字节都执行的一项操作,用于产生位时序和改善频谱质量。

13. 位传输顺序(Int:13,Tag:13)

位传输的顺序,或者最低有效位(LSB)优先,或者最高有效位(MSB)优先。

14. 唤醒过程(Int:14),保留(Tag:14)

该参数(Int:14)应定义 RFID 标签是否需要唤醒过程。唤醒的 RFID 标签可以马上与读写器进行通信。

15. 极化(Int:15,Tag:15)

规定天线发射/接收电磁波的方向。

16. 标签接收机的最小带宽(Tag:16)

标签接收机所能接收频率的最小范围。

注:扩频、FHSS、DSSS 和码片的说明见第 8 章。

10.3 ISO/IEC 18000-3:13.56MHz 频率下的空中接口通信参数

定义了两种相互独立的模式,这两种模式互不兼容。

读写器和 RFID 标签可以支持模式 1(M1)或模式 2(M2),也可以两种模式都支持。两种模式都采用"读写器先讲"机制。

模式 1 中的物理层、防冲突系统和协议采取的方法是和 ISO/IEC 15693 中使用的方法相一致。详细内容参见第 9 章。

10.3.1 模式 2(M2):物理层和空中接口参数

1. 物理层和空中接口参数

(1) 读写器到标签(参阅 10.2 节)如表 10.1 所示。

表 10.1 物理层和空中接口参数:读写器到标签

参 数	参 数 名 称	描述/值
M2-Int:1	工作频率范围	13.56MHz±7kHz
M2-Int:1a	默认工作频率	13.56MHz
M2-Int:1c	工作频率精度	±100ppm
M2-Int:2	占有信道带宽	它们需要满足欧洲电信标准化协会 ETSI(European Telecommunications Standards Institute)和美国联邦通信委员会 FCC(Federal Communications Commission)的管理规范
M2-Int:2a	最小接收机带宽	适合接收标签信道或相关的信道
M2-Int:6	定时	
M2-Int:6a	发送-接收转换时间	0~50μs
M2-Int:6b	接收-发送转换时间	第一类:0~100μs;第二类:取决于应用
M2-Int:6c	读写器发送功率上升时间	0~10μs
M2-Int:6d	读写器发送功率下降时间	0~10μs
M2-Int:7	调制	PJM(相位抖动调制),以非常小的相位差异(±1°~±2°)表示数据 1 和 0
M2-Int:8	数据编码	改进调频制(Modified Frequency Modulation,MFM)
M2-Int:9	位速率	423.75Kb/s
M2-Int:9a	位速率准确度	与载波频率同步
M2-Int:11	前同步码	包括一个 MFM 编码违例

参　数	参 数 名 称	描述/值
M2-Int：11a	前同步码长度	16 位
M2-Int：11b	前同步码波形*	命令标记定义了一个命令的开始和位间隔时间，标记包含 3 个部分(图 10.2)：①9 位有效 MFM 数据同步字符串；②一个不会在正常数据中出现的 MFM 编码违例(由一个 2 位间隔、一个 1.5 位间隔及一个 2 位间隔分开的 4 态变化序列组成)，第 4 次转变的边缘定义为一个位间隔的开始；③定义标记结束的尾随 0
M2-Int：11c	位同步序列	参阅 M2-Int：11b
M2-Int：11d	帧同步序列	参阅 M2-Int：11b
M2-Int：13	位发送序列	最低位优先

注：前同步码采用 MFM 编码。

① 改进调频 MFM 编码规则定义如下。

- 位 1 由位间隔中间状态的变化定义。
- 位 0 由位间隔起始状态的变化定义。
- 紧随位 1 的位 0 没有状态变化。

二进制串 101110001 的 MFM 编码实例如图 10.1 所示，位速率为 423.75Kb/s(f_c/32)，f_c=13.56MHz。位间隔为 2.36μs。

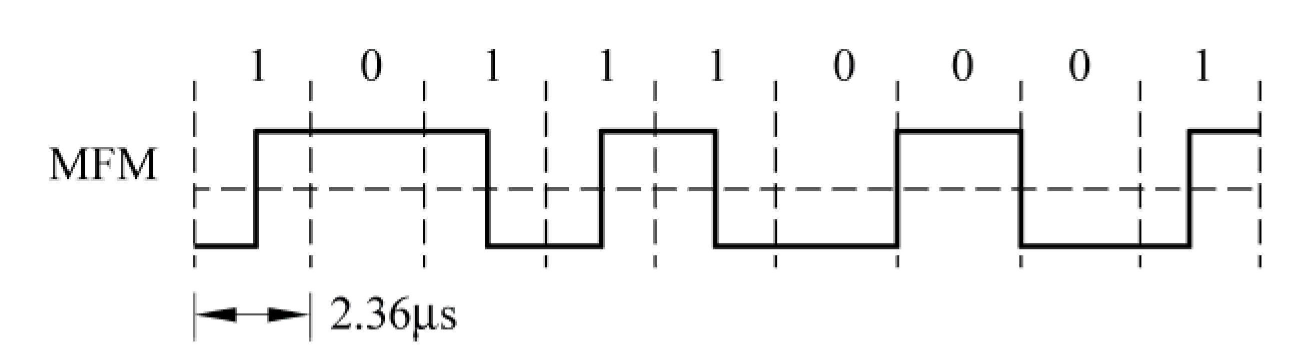


图 10.1　二进制串 101110001 的 MFM 编码

② 前同步码。如图 10.2 所示，第 15 位是编码违例波形。对于正确波形，如果第 15 位为 0，则应在位间隔开始波形发生变化；如果为 1，则应在位间隔中间波形发生变化，但第 15 位都未发生。将图 10.2 中的波形定义为前同步码。

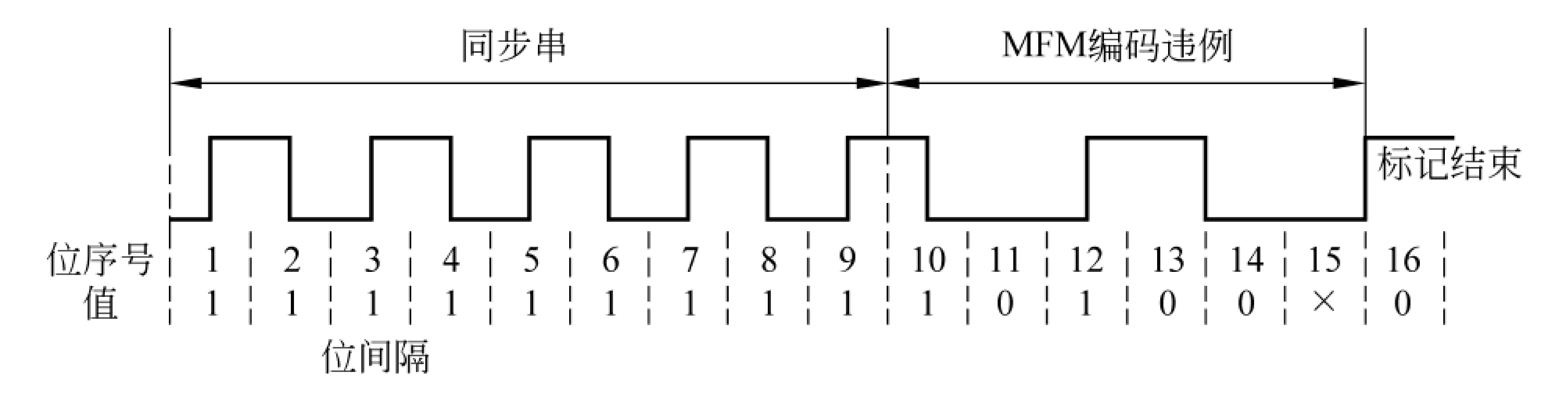


图 10.2　命令或响应标志的前同步码

(2) 标签到读写器如表 10.2 所示。标签是无源的。

表 10.2　标签到读写器链路

Ref.	参 数 名 称	描述/值
M2-Tag：1	工作频率范围	13.56MHz±7kHz
M2-Tag：1a	默认工作频率	不适用于系统不依赖默认工作频率的地方
M2-Tag：1b	工作信道(适用于扩频系统)	标签可从 8 个响应信道中进行选择的多频率工作系统。标签用一个选择信道发送整个响应。标签可能使用 8 个副载波之一。副载波通过对能量场频率分频获得(表 10.3)
M2-Tag：1c	工作频率精度	与载波同步
M2-Tag：1d	跳频速率(适用于跳频[FHSS]系统)	标签在选定的信道上发送整个响应
M2-Tag：1e	跳频序列(适用于跳频[FHSS]系统)	由标签随机选择响应通道
M2-Tag：6	定时	
M2-Tag：6a	发送-接收转换时间	0～200μs
M2-Tag：6b	接收-发送转换时间	50～100μs
M2-Tag：7	调制	负载调制
M2-Tag：7a	扩频序列(适用于直接序列[DSSS]扩频系统)	标签在随机选定的或读写器选定的信道上发送整个响应
M2-Tag：7e	副载波频率	见表 10.3
M2-Tag：7f	副载波频率精度	与载波频率同步
M2-Tag：7g	副载波调制	BPSK(二进制相移键控)
M2-Tag：8	数据编码	MFM(改进调频制)
M2-Tag：9	位速率	105.9375Kb/s
M2-Tag：9a	位速率准确度	与载波频率同步
M2-Tag：11	前同步码	包括一个 MFM 编码违例
M2-Tag：11a	前同步码长度	16 位
M2-Tag：11b	前同步码波形	同 M2-Int：11b
M2-Tag:11c	比特同步序列	参阅 M2-Tag：11b
M2-Tag:11d	帧同步序列	参阅 M2-Tag：11b
M2-Tag:13	位传输顺序	最低位优先

(3) 标签到读写器的通信信号接口。在 BPSK 调制之前进行 MFM 编码。标签使用 8 个可选的调制副载波之一响应。

① 副载波。副载波通过能量场频率的分频获得。信道频率和分频率如表 10.3 所示。

表 10.3　信道频率和分频率

信道	频率/kHz	分频率/kHz	信道	频率/kHz	分频率/kHz
A	969	14	E	2086	6.5
B	1233	11	F	2465	5.5
C	1507	9	G	2712	5
D	1808	7.5	H	3013	4.5

② 调制。基于负载调制。数据采用 MFM 编码,然后以 BPSK 调制方式调制到副载波上。

③ 数据速率。数据传输速率为 106Kb/s(f_c/128),f_c=13.56MHz。位间隔时间为 9.44μs。

2. 标签的识别

以下的内容是为 10.3.2 节和 10.3.3 节准备的。

多标签的识别是通过 FTDMA(频分和时分多址)的方式来实现的。有 8 个响应信道可供标签使用,每个标签随机选择一个信道响应有效命令,响应通过所选信道传输一次。

除了随机选择信道外,标签还能够随机静默响应(有关静默的概念见 10.3.2 节)。当一个响应被静默后,标签不传输该响应。当识别大量标签时,随机静默是必需的。所有 FTDMA 频率和时间参数都通过命令来定义。

所有的命令都有时间戳。标签存储进入读写器工作场后接收到的第一个时间戳。

10.3.2　模式 2(M2):命令与响应

1. 命令格式

命令格式如表 10.4 所示。表中各字段(符号)的含义如表 10.5 所示。

表 10.4　有效的命令格式

项　　目	起始字段	标识符字段	地址及长度字段	数据	CRC
群读	F[Cd] Cn	G Ci	[R]或[Ra Rl]		C
特殊读	F[Cd] Cn	SS	[R]或[Ra Rl]		C
群读/写	F[Cd] Cn	G Ci {PPP}	[RW]或[Ra Rl Wa Wl]	D	C
群特殊读/写	F[Cd] Cn	SS {PPP}	[RW]或[Ra Rl Wa Wl]	D	C

表 10.5　命令格式表中各字段的含义

编码	字　　段	位	注　　释
F	标记	16	MFM 违例序列
Cn	命令	16	命令字段,定义读/写命令和信道/静默比
Cd	命令编号	16	命令编号字段

续表

编码	字　段	位	注　释
SS	特殊标识符	32	标识符字段
G	应用组标识符	16	标识符字段
Ci	条件标识符	16	标识符字段
PPP	口令	48	口令
R	读地址和长度	16	存储器读的 8 位地址和 8 位长度字段
W	写地址及长度	16	存储器写的 8 位地址和 8 位长度字段
Ra	读地址	16	存储器读的 16 位地址
Rl	读长度	16	存储器读的 16 位长度字段
Wa	写地址	16	存储器写的 16 位地址
Wl	写长度	16	存储器写的 16 位长度字段
D	写数据	—	将被写的数据
C	CRC	16	CRC 验证

注："[]"中的内容是可选的。

最小的命令长度为 112 位。

1）起始字段

（1）标记字段 F。标记字段包含一个在正常的数据中不会有的 MFM 违例。该字段指示命令的开始。

（2）命令字段 Cn。

信道/静默比。信道/静默比用于确定选择信道或静默。

对于有效的随机信道命令：

① 如果选择了非静默，则标签在随机选择的信道上传送响应。

② 如果选择为 1/2 静默～511/512 静默，标签随机选择传输（非静默）或不传输（静默）响应。命令中提供的静默比（1/2、3/4、7/8、31/32、127/128 或 511/512 静默）决定标签被静默的概率。如果选择 3/4 静默，则标签在整个工作期间，按 3 次静默、1 次传送的概率进行。

③ 如果选择完全静默，则标签不响应，标签将被设置为暂时静默状态。暂时静默状态的标签只能响应具有新的读写器标识符的命令，见下面的"（3）命令编号"。

（3）命令编号 Cd。

命令编号用于设定本地时间戳及识别读写器。

当标签进入一个新的读写器工作区域时，标签将存储接收到的第一个有效命令的时间和读写器的编号。

2）标识符字段 SS、G、C_i

命令中的标识与标签中存储的用于通信的标识符相同时，该命令才有效。

口令字段(PPP)用于限制标签存储器的读写操作。

3) 地址和长度字段 R、W、Ra、Rl、Wa、Wl

该命令字段确定命令包含的是 8 位地址和 8 位长度字段还是包含 16 位地址和 16 位长度字段。地址和长度字段定义了存储器读写的字起始地址和长度。

4) 数据

数据在写命令时存在。

2. 响应格式

响应格式如表 10.6 所示,所有字段都是最低有效位优先传输。对于多字节字段,最低有效字节的最低有效位定义该字段的最低有效位。

表 10.6　有效响应格式

响应类型	开始字段	系统存储器字段	数据	CRC
正常响应	F [H] T	L M SS G Ci Co	[D]	CC
短响应	F T	SS	[D]	CC

表 10.6 中各符号的意义为:F,前置同步码;H,硬编码;T,时间戳;L,锁定指针;M,生产编码;SS,特殊标识符;G,应用组标识符;Ci,条件标识符;Co(Cw),配置字;D,读数据;CC,CRC 校验码。[]中的内容是可选的。

响应的最小长度为 96 位。

硬编码指出标签的存储器的容量和存储块的大小。

10.3.3　模式 2(M2):防冲突管理

1. 总体描述

多标签识别使用频分多址和时分多址(Frequency and Time Division Multiple Access,FTDMA)的组合来实现。

标签有 8 个可用响应信道。在响应有效命令时,每个标签随机选择一个传输响应的信道。仅使用所选择的信道传输一次响应。接收到下一个有效命令时,每个标签随机选择一个新的信道传输响应。对随后的有效命令,重复使用这种利用随机信道选择进行响应的方法。可以在不同信道上同步接收多标签的响应。

2. 响应信道

系统使用在 969～3013kHz 的 8 个响应信道。对于不同的读写器类型和不同的标签数量,可以使用不同的响应模式来提高标签识别速率。标签使用的响应模式可以通过读写器来选择。

3. 响应模式

响应模式可分为固定信道响应模式和随机信道响应模式。其中,随机信道响应模式又分为以下 3 种。

(1) 非静默响应模式。

(2) 随机静默响应模式。

(3) 完全静默响应模式。读写器可以将标签设置为完全静默响应模式。在该模式下,标签不响应从同一读写器发出的命令,因此也不会与其他标签响应发生冲突。该模式可用于多标签情况下,改进标签识别率。当标签进入一个新的读写器范围内,它将退出完全静默模式。

当标签使用随机信道响应模式或随机信道及随机静默响应模式时,为了避免在某信道上长时间不传输信息,标签应包含一种方法使得在其他信道产生若干个(如 15 个)非静默响应后,强制在该信道上进行响应。

4. 防冲突管理

在响应有效命令时,每个标签随机选择一个传输响应的信道,传输一次响应。如果冲突,则在接收到下一个有效命令时,每个标签再随机选择一个新的信道传输响应。对随后的有效命令重复使用这种利用随机信道选择进行响应的方法。

除随机信道选择外,标签还可随机静默单个响应。当响应被静默后,标签将不发送这个响应。随机静默在识别大量标签时是必要的,因为可减少响应的标签数,降低冲突的概率。一旦标签被识别,它将暂时被命令静默,退出防冲突。

10.4 ISO/IEC 18000-6:860～960MHz 频率下的空中接口通信参数

10.4.1 概述

本节描述了一个反向散射 RFID 系统,支持有电池或无电池两种标签。

标签接收读写器传来的幅度调制信号。标签对标签天线终端的射频负载阻抗进行调制。

工作在 860～960MHz 的工业、科学与医学频段,具有两种类型的模式(类型 A 和类型 B)。两种类型都采用相同的返回链路(即标签发回的响应)。类型 A 在前向链路(读写器向标签发信号)中采用了脉冲间隔编码(Pulse Interval Encoding,PIE)及时隙冲突仲裁算法,类型 B 在前向链路中使用曼彻斯特编码及二进制树冲突仲裁算法。两种类型的技术差别细节如表 10.7 所示,返回链路都采用 FM0 编码。

表 10.7 类型 A 和类型 B 的对比

参 数	类 型 A	类 型 B
前向链路编码	PIE	Manchester
调制指数	27%～100%	18%或 100%
数据速率	33Kb/s (平均)	10Kb/s 或 40Kb/s (根据本地规范)
返回链路编码	FM0	FM0
冲突仲裁	时隙	二进制树
标签唯一标识符	64 位(40 位 SUID)	64 位
标签寻址能力	8KB	2KB

续表

参　数	类 型 A	类 型 B
存储器寻址	块,大小可达 256 位	字节块,可以写入 1、2、3、4 字节
前向链路差错检测	所有命令均有 5 位 CRC(所有长命令另附 16 位 CRC)	16 位 CRC
返回链路差错检测	16 位 CRC	16 位 CRC
冲突仲裁线性度	可达 250 个标签	可达 2^{256} 个标签

10.4.2　参数表

表 10.8 和表 10.9 给出了类型 A 和类型 B 的参数。

表 10.8　读写器到标签链路参数

读写器到标签	参 数 名 称	说　　明
Int：1	工作频率范围	860～960MHz
Int：1a～5	默认工作频率……	与当地无线电规则一致
Int：6a	发送到接收的转换时间	读写器发射/接收设定时间不应超过 85μs
Int：6b	接收到发送的转换时间	由通信协议规定,参见 Tag：6a
Int：6c	读写器发射功率上升沿时间	最长 1.5ms
Int：6d	读写器发射功率下降沿时间	最长 1ms
Int：7	调制	幅度调制
Int：7d	调制指数	类型 A：标称 30%～100%;类型 B：标称 18%或 100%
Int：7e	占空比	与当地无线电规则一致
Int：9	位速率	类型 A：33Kb/s,受当地无线电限制; 类型 B：10Kb/s 或 40Kb/s,受当地无线电限制
Int：9a	位速率精度	100ppm
其他	前同步码……	在本章相关处介绍

表 10.9　标签到读写器的链路参数

标签到读写器	参 数 名 称	说　　明
Tag:1	工作频率范围	860～960MHz
Tag:1a	默认工作频率	标签在 Tag:1 指定的频率范围应响应读写器信号

续表

标签到读写器	参 数 名 称	说　　明
Tag:1b	工作信道(针对扩频系统)	标签在 Tag:1 指定的频率范围应响应读写器信号
Tag:2～5	占有信道带宽……	与当地无线电规则一致
Tag:6a	发送到接收的转换时间	类型 A:标签应在其响应结束后的两个位时间内开启接收命令窗口; 类型 B:400μs
Tag:6b	接收到发送转换时间	类型 A:150～1150μs;类型 B:85～460μs
Tag:7	调制	后向双态幅度调制
Tag:8	数据编码	双相间隔(Frequency Modulation0,FM0)
Tag:9	位速率	典型的 40Kb/s 或 160Kb/s 返回链路数据速率为前向链路数据速率的 4 倍
Tag:9a	位速率精度	±15%
其他	前同步码……	在本章相关处介绍

10.4.3 FM0 返回链路(适合于类型 A 和类型 B)

1. 数据编码

数据编码采用 FM0 技术。

在 FM0 编码中,波形(电平)变化发生在所有的位边界和被发送的逻辑 0 的位中间。

数据编码为最高有效位优先,图 10.3 所示为 8 位编码。

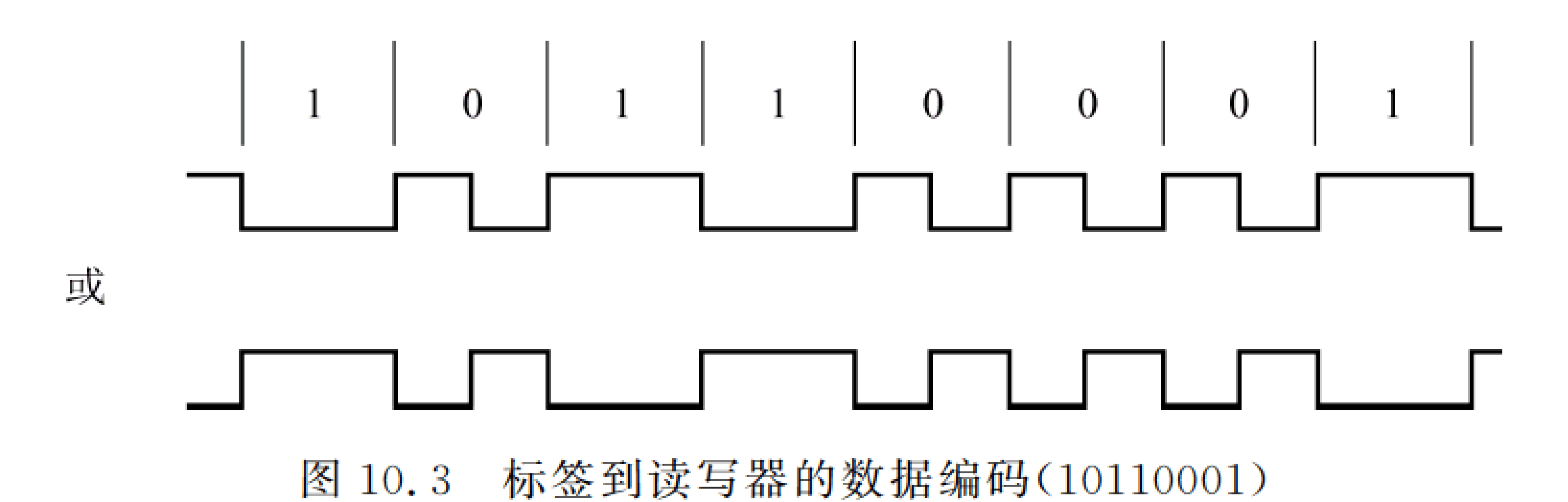


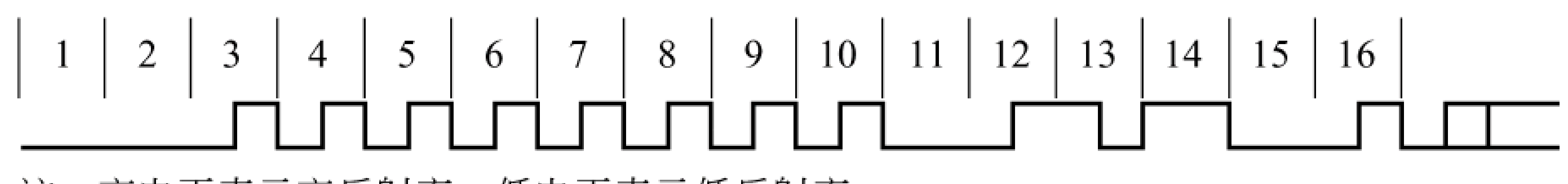
图 10.3　标签到读写器的数据编码(10110001)

2. 信息格式

返回链路信息由前同步码引导下的 n 个数据位组成。数据位传送为最高有效位优先。

前同步码包含图 10.4 所示的 16 位,包含多种代码违例形式(相关序列不同于 FM0 规则)。

将标签调制器的开关从高阻抗状态切换到低阻抗状态时,引起入射能量的改变以进



注：高电平表示高反射率，低电平表示低反射率

图 10.4　前同步码波形

行反向散射。

10.4.4　类型 A 前向链路(编码、数据元、协议和冲突仲裁)

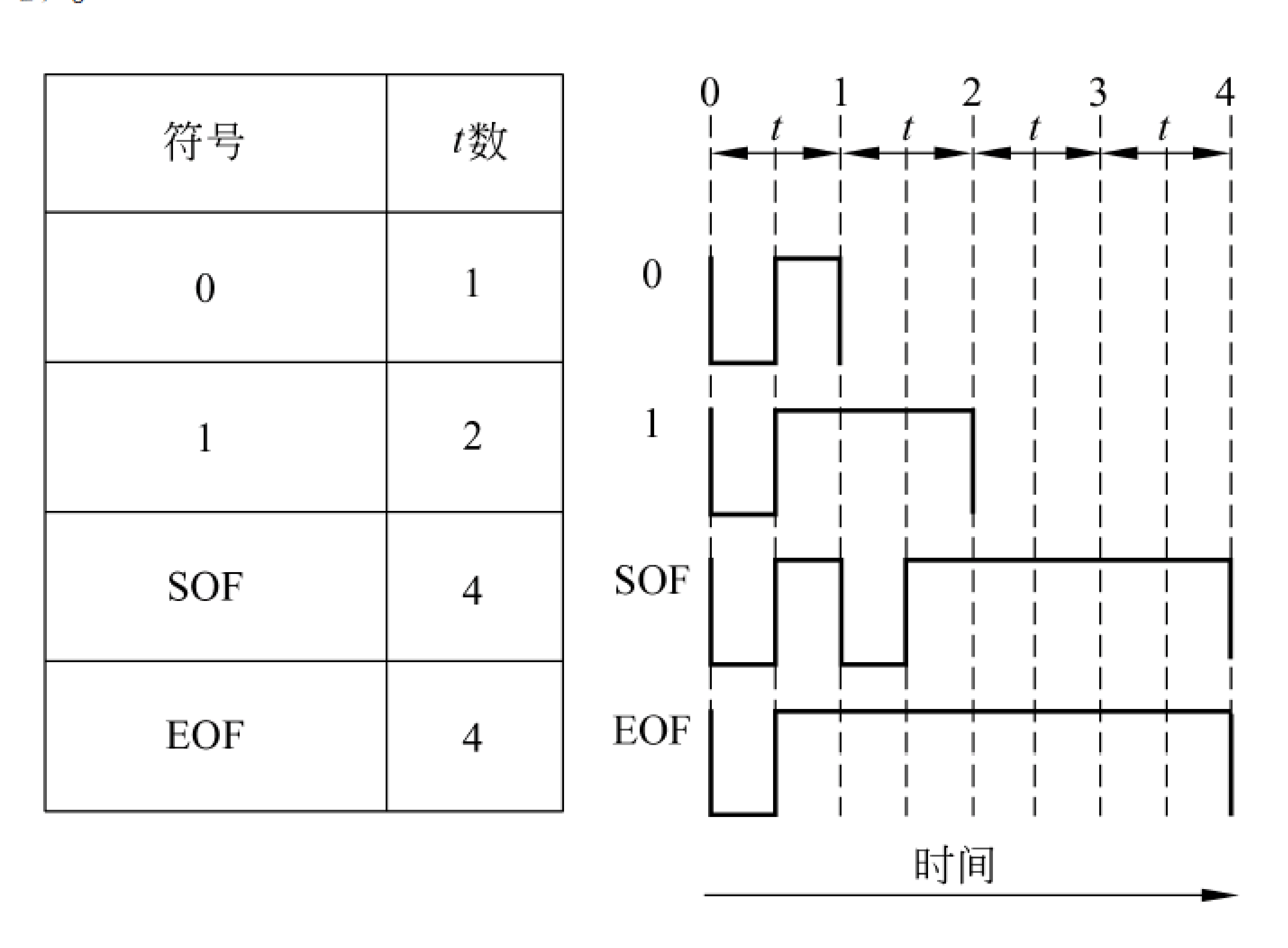
1．PIE 前向链路

1）载波调制脉冲

从读写器到标签的数据传输是通过调制载波振幅完成的。

2）数据编码及帧形成

图 10.5 中的时间参数 t 规定了代表读写器发射符号 0 的两个连续脉冲下降沿之间的参考间隔(20μs)。



符号	t数
0	1
1	2
SOF	4
EOF	4

图 10.5　PIE 符号

图 10.5 中定义了 4 个符号,符号参考了间隔 t,持续时间为 $1t$、$2t$ 和 $4t$,容差范围为±100ppm。

3）帧格式

在发送帧之前,读写器先确保已建立的未调制载波持续时间已超过 300μs(静默时间)。

帧由帧起始、数据位和帧结束组成。读写器发出帧结束之后按协议要求保持发射一个平稳的载波,这样标签可被激励以便发射其响应。

2．类型 A 数据元

1）唯一标识符

标签的唯一标识符应采用表 10.10 和 ISO/IEC 15963 指定的形式。

表 10.10　UID 格式

MSB			LSB
$b_{64}..b_{57}$	$b_{56}..b_{49}$	$b_{48}..b_{33}$	$b_{32}..b_{1}$
'E0'	IC 制造商代码	RFU,设置为 0	IC 制造商确定的序列号

如果使用 UID，IC 制造商应按照表 10.10 永久设置 UID。

2）子唯一标识符 SUID

在很多的命令和在冲突仲裁处理的标签响应中，只有一部分称为子 UID(SUID)的被传送。返回完整的 64 位 UID 的获取系统信息命令除外。

SUID 包含 40 位：8 位制造商代码后跟一个序列号 32 位。

3. 类型 A 协议元素

1）标签存储器结构

假定物理存储器以固定大小的块组成。可寻址多达 256 个块,块的大小可多达 256 位,由此得到的标签最大存储器容量为 8KB(64K 位)。

2）标签签名

标签签名由 4 位组成,标签可以通过若干机制生成签名。例如,通过一个 4 位伪随机数发生器,或者通过 SUID。在冲突仲裁过程中,读写器可在发送的命令中包含签名,只有签名匹配的标签才会响应这些命令。

4. 类型 A 协议描述

1）命令格式

两种命令格式,即 16 位短命令及长命令。

(1）短命令格式。短命令由下面所定义的字段组成。协议扩展位＝0。

SOF	协议扩展	命令码	参 数	CRC-5	EOF
	1 位	6 位	4 位	5 位	

(2）长命令格式。长命令由下面定义的字段组成。协议扩展位＝1。

SOF	协议扩展	命令码	参 数	CRC-5	SUID（可选）	数据	数据（可选）	CRC-16	EOF
	1 位	6 位	4 位	5 位	40 位	8 位	8～n 位	16 位	

数据(可选)字段长度的值被定义为 n，这里 $n=m+8$，m 是在标签存储器中编程的位数。当前，$m=32$,协议允许 m 值最大到 256。

2）命令参数

命令参数字段的最高有效位是 SUID 标志。其余 3 位是轮询周期的编码。

轮询周期使用 3 位编码(命令参数字段的低有效位),其与时隙数的关系如下。

位编码	000	001	010	011	100	101	110	111
时隙数	1	8	16	32	64	128	256	RFU

3）命令码定义和类别

命令码的长度为 6 位。定义了 4 个命令集，分别为强制的、可选的、定制的及专用命令，共 18 条命令。强制命令仅有 4 条。

4）响应格式

来自标签的一般响应格式如下。其中参数和数据字段在介绍每一个命令中定义。

前同步码	出错标志	〔参数〕	〔数据〕	CRC-16

出错标志由两位组成，b_1 表示是否有错（$b_1=0$ 为无错；$b_1=1$ 为有错），b_2 为 RFU。当错误代码被置位时的响应格式如下。

前同步码	出错标志	〔错误代码〕	终止位
	2 位	4 位	

5）冲突仲裁

冲突仲裁采用了一种轮询和时隙的机制。一次轮询由多个时隙组成，每个时隙有一个足够长的持续时间以便读写器接收标签的响应。由读写器来决定一个时隙实际的持续时间。轮询中的时隙数被称为轮询周期大小，由读写器来决定。在冲突仲裁过程中，读写器基于本次轮询中的冲突次数动态地选择一个最佳的下一轮轮询周期的时隙数。

在轮询开始时，标签选择一个响应时隙，响应时隙选择由伪随机数发生器决定，在一个轮询周期内该响应时隙保持不变。

在标签的响应里包括 4 位标签签名。

在读写器发出轮询开始命令后，可能出现如下 3 种结果。

（1）读写器没有收到响应，因为没有一个标签选择时隙 1，或者读写器没有检测到标签的响应。

（2）读写器检测到两个或多个标签响应之间的冲突。

（3）读写器收到一个无冲突的标签响应。该标签退出本轮询的冲突仲裁。

然后将时隙计数器加 1（在读写器内有一个时隙计数器，其初始值为 1）。当时隙计数器等于标签先前选择的时隙号时，该标签根据上述规则发送响应。

一次轮询一直持续到所有的时隙都被检测到为止。如果还存在冲突的标签，则进入下一次轮询。

10.4.5　类型 B 前向链路（编码、数据元、协议和冲突仲裁）

1. 物理层和数据编码

1）载波调制

从读写器到标签的数据传送通过载波调制完成，数据采用曼彻斯特编码。

调制幅度：① 90%～100%（标称值 100%），通信速率为 40Kb/s。

② 15%～20%（标称值 18%），通信速率为 8Kb/s。

2）协议概念

对于标签到读写器的通信(返回链路)，数据采用反向散射技术发送。这就要求在返回链路中读写器应向标签提供稳定的功率。当读写器激励标签时，标签改变其前端的有效阻抗，从而改变读写器所能看到的标签的射频反射信号。在该时间内，读写器不调制载波，向标签提供稳定的功率。

在所有字节字段中，最高有效位首先传送，顺次到最低有效位。在所有字(8 字节)数据字段中，应首先传送最高有效字节。

3）命令格式

通用命令格式如下。

前同步码检测	前同步码	分隔符	命令	参数	数据	CRC-16

(1) 前同步码检测字段。前同步码检测字段由一个稳定的载波组成(无调制)，持续时间至少 400μs，对于 40Kb/s 的通信速率，该字段为 16 位。

(2) 前同步码。前同步码等于 9 个 NRZ 格式的曼彻斯特码：010101010101010101。其中，2 个数字 01 表示 1 位数，分别为位周期的前半周期和后半周期的电平。

(3) 分隔符。分隔符有多处不符合曼彻斯特编码规则，从而可与正常编码区分。

(4) 命令、参数、数据由各条命令具体规定。

4）响应格式

一般响应格式如下。

返回前同步码	数据	CRC-16

当标签收到一个写命令，它应执行写操作，应该有一个等待时间(至少为 15ms)，为写入 E^2PROM 提供必要的时间。

图 10.6 所示为一个写命令的操作序列。紧跟写等待时间，读写器发出一个标签再同步信号。该信号由 10 个连续的 01 信号组成。标签再同步信号的目的是初始化标签数据恢复电路。在完成一个写操作后需要再同步信号，因为读写器在写等待的时间内有可能输出一些虚假信号。如果没有标签再同步，标签有可能因虚假信号而造成错误的校准。

动作	写命令	响应	写等待	标签重新同步	下一条命令	响应
执行操作方	读写器	标签	读写器	读写器	读写器	标签

图 10.6　写命令的操作序列

2. 数据元素的定义

1）唯一标识符

ISO/IEC 定义的唯一标识符如下。

MSB		LSB
'E0'	根据 ISO/IEC 7816-6 分配的 IC 制造商代码	芯片制造商分配的 48 位
字节 0	字节 1	字节 2……字节 7

2）标签存储器组织结构

以单字节的形式组成块，寻址可达 256 块。由此导出最大的存储器容量为 2KB(允许扩充)。

3）块安全状态

每一个字节有一个对应的锁定位。

3. 标签状态

标签具有如下 4 个主要状态。

(1) 断电(POWER-OFF)：当读写器不能激励标签时，标签所处的状态(对于电池辅助支持的标签，该状态意味着 RF 激励电平尚不足以开启标签的电路)。

(2) 就绪(READY)：当读写器首次激励起标签后，标签即处于此状态。

(3) 识别(ID)：当标签允许被读写器识别时所处的状态。

(4) 数据(DATA_EXCHANGE)：当标签被读写器识别并选中时，标签处于此状态。

4. 冲突仲裁

为了冲突仲裁，标签需要以下两个硬件。

- 一个 8 位的计数器 COUNT。
- 一个 1 位的随机数生成器(产生 0 或 1 两个可能值)。

一开始通过命令将一组标签置入 ID 状态，并将标签的计数器置为 0。

经过上面描述的选择后，接下来将执行以下循环。

(1) 所有计数器 COUNT 为 0 的处于 ID 状态的标签应发送其 UID。

(2) 如果有多于一个标签进行发送，读写器会收到冲突响应，则发送一个命令，对标签进行操作，进入步骤(3)。

(3) 若标签 COUNT 计数器不等于 0，应增加 COUNT 计数器值(加 1)，即它们被推迟发射。

若计数器为 0(这些标签是刚发送过响应的)将生成一个随机数(1 或 0)。那些生成为 1 的标签将增加 COUNT 计数器内容并且不发送 UID；那些生成为 0 的标签将保持 COUNT 计数器为 0，并再次发送它们的 UID。

现在 4 种可能性之一的情况将会发生。

① 如果多于一个的标签发送，则应发送命令，返回步骤(2)。(可能性 1)

② 如果所有标签生成为 1，没有发送，读写器什么也没有收到。读写器发送命令将所有标签计数器减 1，计数器为 0 的标签进行发送。这种情况将返回步骤(2)。(可能性 2)

③ 如果只有一个标签发送 UID，且读写器验证接收正确，该标签将进入 DATA_EXCHANGE 状态，并且发送其数据，返回步骤(1)。

读写器发送命令，将处在 ID 状态的标签计数器 COUNT 减 1。(可能性 3)

④ 如果只有一个标签发送 UID,并且读写器验证收到有错,读写器将发出命令让标签重复发送一次。如果 UID 号收到正确,返回步骤(3)。如果该 UID 号又被重复收到多次(该次数可以根据系统所期望的错误处理等级设定),可以认定有多个标签在发送,返回步骤(2)。(可能性 4)

标签内 8 位 COUNT 计数器与一位随机数的说明如下。

① 在冲突仲裁过程中,各标签内的 COUNT 值不会完全相等,而且仅有处于 ID 状态,而且 COUNT=0 的标签才能响应读写器发来的相关命令,给出唯一标识符 UID。

② 如果场内有多张标签,而且冲突严重,则会多次进行 COUNT+1 和 COUNT−1,其目的是分别减少返回 UID 的标签数(加 1),或者在仲裁后期因为在场内参与仲裁的标签减少而让它们向 COUNT=0 的方向变化。

5. 命令

命令有 4 种类型:强制命令、可选命令、定制命令和专用命令。

在 ISO/IEC 18000 国际标准中介绍了强制命令和可选命令,而且主要涉及冲突仲裁和读/写标识中存储器的内容。

10.5 ISO/IEC 18000-7:433MHz 频率下的有源标签空中接口通信参数

10.5.1 物理层

- 载波频率:433.92MHz;精度:±20ppm。
- 调制类型:FSK。
- 频率偏离:50kHz;上限:f_c+50kHz;下限:f_c−50kHz。
- 位速率:27.7Kb/s;精度:±200ppm。
- 唤醒信号:30kHz。

唤醒信号是一个持续 2.5~2.7s 的 30kHz 副载波,检测到唤醒信号的所有标签将进入就绪状态等候读写器的命令。

10.5.2 数据、命令和冲突仲裁

1. 总则

标签与读写器之间的数据以包的格式传输,一个包由前同步码、数据字节和最终逻辑低电平组成。前同步码的结束和数据首字节的开始由前同步码最后两个脉冲指示。传输顺序是最高有效字节优先。每一个字节最低有效位优先。图 10.7 所示为一个包的前同步码和首字节的数据 00100110('64')通信时序。

(1) 前同步码。前同步码是由 20 个周期为 60μs 的脉冲组成,30μs 高电位,30μs 低电位,后面是最终同步脉冲,用来识别通信方向:40μs 高,54μs 低(标签到读写器);54μs 高,54μs 低(读写器到标签)。

(2) 数据字节格式。数据字节是曼彻斯特码的格式,由 8 个数据位和 1 个停止位组

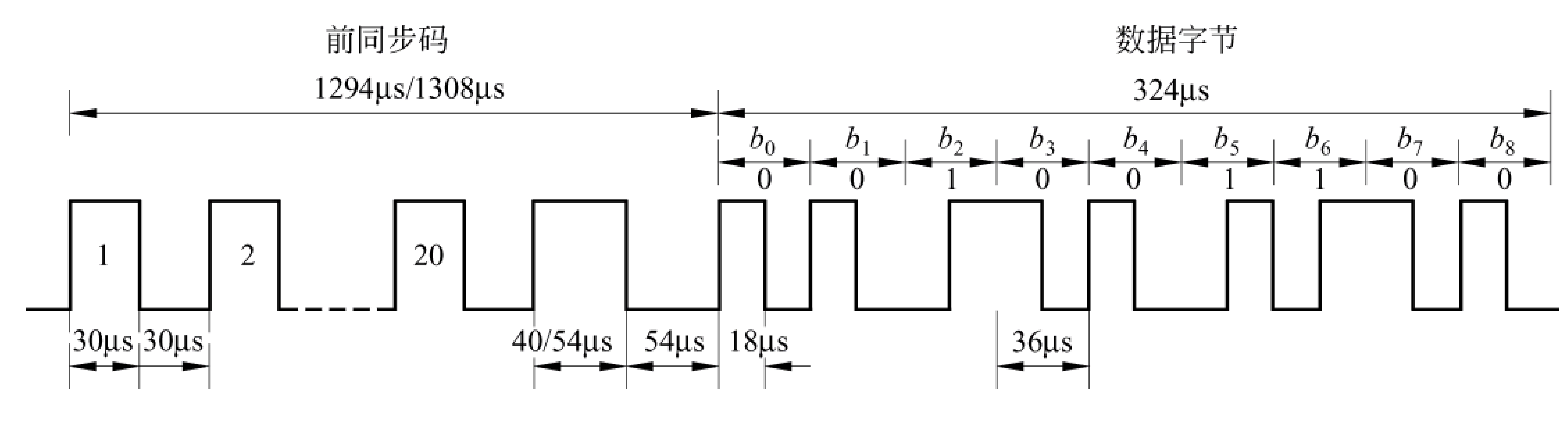


图 10.7　数据通信时序

成,每一位周期为 36μs,整个字节周期为 324μs。位时间中心的下降沿表示位 0,而上升沿表示位 1,停止位用位 0 编码。

(3) 包结束期。每一包 CRC 字节结束后传送一个 336μs 连续逻辑低的结束周期。

2. 读写器-标签命令格式

标签应识别的命令格式如下。

MSB　　　　　　　　　　　　　　　　　　　　　　　　LSB

命令前缀	命令类型	所有者 ID	标签 ID	读写器 ID	命令代码	参数	CRC
1	1	3	4	2	1	n	2 字节

所有者 ID、标签 ID 和参数字段的存在由命令类型和命令代码确定。

1) 命令类型(表 10.11)

表 10.11　命令类型字段

b_7	b_6	b_5	b_4	b_3	b_2	b_1	b_0
预留	预留	预留	预留	预留	1	0=广播(标签 ID 字段不存在) 1=点对点(标签 ID 字段存在)	0=所有者 ID 字段不存在 1=所有者 ID 字段存在

广播是指采集场内在某一范围内的全部标签 ID,点是指某个标签,ID 为标识符。

2) 所有者 ID

所有者 ID 字段存在时,只允许读写器与属于特定所有者 ID 组里的标签进行通信。所有者 ID 可以被修改。如果标签没有使用所有者 ID 或是它的值被置为 0,标签应响应任何一个在命令信息中不包含所有者 ID 的读写器命令。

3) 标签 ID

标签 ID 是在制造过程中唯一分配给每个标签的 32 位整数,这个数字不能被修改,是只读的。

4) 读写器 ID

读写器 ID 是 16 位整数,可以修改。

5) 命令

有以下 3 类命令,完成的功能如下:

① 采集场内所有标签 ID(或在某些指定领域内)。

② 读/写存储器。

③ 设置密码、解除密码等。

3. 冲突仲裁

读写器发送采集命令，标签随机选择时隙进行响应。采集周期由若干个时隙组成，一个周期内所有时隙都被访问过。采集周期结束时，读写器将该周期内采集到的标签进入休眠状态，在随后的采集周期不再参与采集。

冲突仲裁经过若干个采集周期，直到场内所有标签 ID 被采集为止。

10.6 智能卡、RFID 涉及的国际标准和专利

1. 计算机和小型微处理器

计算机和小型微处理器已普及到科研、政府、行业和生活中各个方面，其本身是以数字方式进行处理和运算的，或者嵌入到各个领域的设备中，并可通过网络与外界联系和通信。目前已从有线向无线方向发展、推广。

本书从介绍智能卡与 RFID 的硬件出发，在第 8 章中重点讨论了无线通信技术以及数字和射频信号之间的联系及工作原理。在第 9 章和第 10 章分别讨论了非接触式 IC 卡(无线)和 RFID 标签的空中接口和相关的国际标准，涉及的主要内容包括数字编码、射频信号的调制、防冲突、命令系统及运行状态的转换等，为进入最终的服务目标作好准备。

2. 国际标准

在 IC 卡和 RFID 标签中即使工作在同一频率范围内也存在多个国际标准。例如，在 13.56MHz 频率下的国际标准有 ISO/IEC 14443(Type A 和 Type B)、ISO/IEC 15693、ISO/IEC 18000 等，还存在其他国际标准化组织制定的标准和各国制定的国家标准。查阅相关资料，发现它们的数字编码、调制和冲突仲裁的方法都不相同，造成命令的巨大差异等，这不仅是因为科技的发展和人类的智慧造成的，而且与经济利益有关。一般当新的国际标准宣布时，或者有技术、产品的创新时，往往已申请了多项专利，也可能有多个单位组成不同的团体而同时或先后向国际标准化组织提出他们的国际标准的申请。

3. 专利

国家知识产权局是我国主管全国专利工作和涉外知识产权事宜的机构。

专利权是指专利权人对发明创造享有的专利权，即国家依法在一定时期内授予发明创造者或其权利继承者独占使用其发明创造的权利，非专利权人想使用他人的专利技术，必须依法征得专利权人的授权或许可。无论是申请专利或获得授权都要付费。

专利的基本特征为“独占”与“公开”。公开是指社会公众可通过正常渠道获得专利授权，据统计全世界每年 90%～95%的发明创造成果可在专利文献中查到。独占是指技术发明人在一段时间内享有排他性的独占权利。

我国将专利分为 3 种：发明、实用新型和外观设计。发明专利权期限为 20 年，其他专利权限为 10 年。当一项发明创造向国家审批机关提出专利申请，并获得核准后，才能获得专利权。

习题

1. ISO/IEC 18000 国际标准中规定的标签使用在哪几个频段？为什么在有些频道中发射功率要受当地管理机构限制？
2. 什么是有源标签？什么是无源标签？各有什么优、缺点？
3. 在 ISO/IEC 18000 国际标准中，一般情况下，哪些命令的功能是共同具备的？在同一频段中，不同模式的命令格式又各不相同，原因是什么？
4. 与 ISO/IEC 7816 相比，在命令系统方面，ISO/IEC 18000 还有哪些不足？
5. 前同步码中的违例码起什么作用？
6. 防冲突处理的主要目的是什么？请总结在 ISO/IEC 14443 和 ISO/IEC 18000 标准中采用了哪几种防冲突机制？其共同点是什么？
7. ISO/IEC 18000 国际标准规定的各频段下的 RFID 系统工作原理是否相同？识读距离是否相同？
8. 唯一标识符在空中接口通信协议中的作用是什么？有哪几种格式？遵循什么标准进行分配？
9. 国际标准的制定与专利权的实施对卡和标签有什么影响？
10. 卡与标签的标准制定对物联网的应用起什么作用？

第 11 章　读写器结构和系统的测试

读写器在系统中起着重要的作用，是负责正确读写卡（或标签）信息的设备。根据应用的需求，它可以是负责和控制卡（或标签）任务的独立设备，具有读写显示和数据处理等功能；也可以在计算机或网络系统指挥下完成操作，并提供下列信息以实现多个读写器在网络系统中的运行：本读写器的识别码、读出或写入信息的日期和时间，读出或写入的信息等。同时要保证信息的传送和操作的安全。

读写器和卡（或标签）之间的所有操作都由应用软件来指挥完成，在计算机系统结构中，应用软件作为主动方对读写器发出命令，而读写器作为被动方返回应答信息。读写器接受命令后，除了一部分命令在读写器中完成外，大部分命令的功能在卡（或标签）内完成。并在卡或标签 COS 的安排下进行处理，返回响应给读写器。在这个过程中，读写器变成了主动方，卡（或标签）则是被动方。

11.1　读写器的组成

IC 卡和射频识别读写器的种类很多，有固定式、便携式、接触式与射频空中接口等形式。功能上由于不同的应用需要，差异也很大，但就其对卡和 RFID 标签的操作功能来说，一般应具备以下几个基本功能。

（1）接触式 IC 卡的插入/退出的识别与控制；IC 卡或标签进/出射频区的识别、防冲突和控制。

（2）向无源的 IC 卡或标签提供其所需的稳定电源，或者发送射频信号传送能量。

（3）实现与卡或标签的数据交换，并提供相应的控制信号；读写器发出命令、接收响应。

（4）对于加密数据系统，应提供相应的加密解密处理及密钥管理机制。

（5）读写器与卡、标签的相互认证。

（6）持卡人的身份识别。

1. 读写器的总体结构

读写器可以是一个独立面向应用的应用机具，或者以从设备方式（或称外部设备）与主设备（一般为微机）一起构成一个 IC 卡应用机具。前者一般以简单专用设备方式出现，如水、电和煤气等的 IC 卡计费设备，IC 卡自动售票机，IC 卡付费电话，IC 卡自动售货机等，这些机具的使用方式与功能均在出厂前由厂家制备好，使用仅能根据不同的情况进行小范围设定；后一类设备在功能上仅完成面向 IC 卡的操作，但以丰富而又灵活的应用接口给应用开发者提供了良好的支持，一般还与网络相连，是系统应用中一个非常实用的选择。

接触式 IC 卡读写器的组成如图 11.1 所示，它由 IC 卡适配插座（简称 IC 卡座）、IC 卡电气接口电路、用于 IC 卡时序生成与数据交换的微处理器及与其他主设备（如果需要）的连接接口等部分组成。

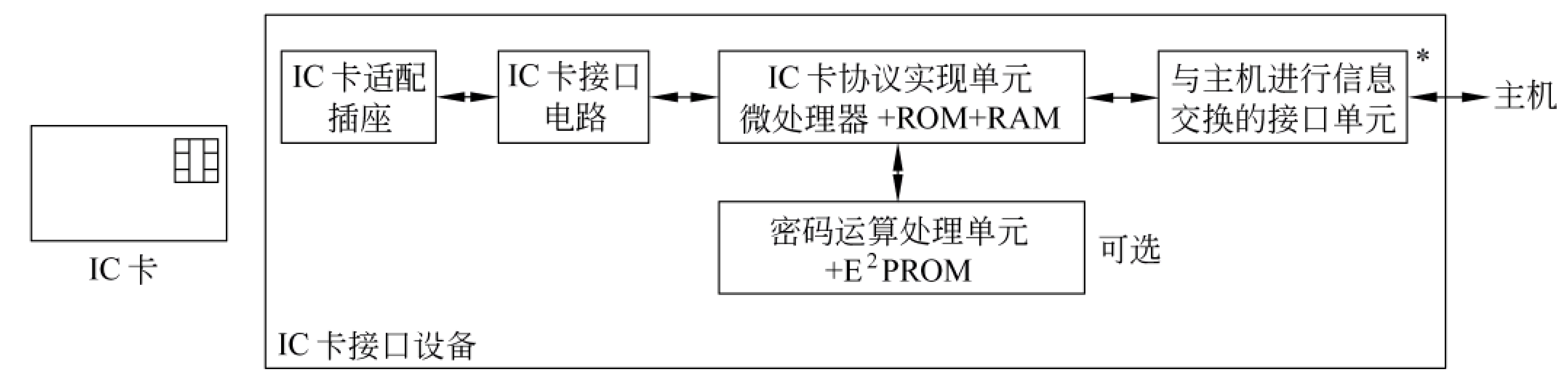


图 11.1　接触式 IC 卡读写器总体结构框图

非接触式 IC 卡或标签无触点，读写器不需要 IC 卡适配插座。但需要设置天线和调制解调器，发送/接收射频信号，向 IC 卡或标签传送能量，并进行双向数据传送，假如场内有多个卡或标签存在，则必须进行冲突仲裁。

双界面卡和标签的读写器兼有接触式和非接触式两方面功能。

2. IC 卡适配插座

用于接触式 IC 卡的适配插座是构成 IC 卡与读写器间的物理连接的部件。由于涉及插入时的手感及插拔寿命要求较高，IC 卡座在设计和制造中比普通接插件的要求高，难度也较大。

1）IC 卡适配插座的结构形式

各厂家为迎合各类不同的使用需要，推出了多种多样的 IC 卡适配插座以供选用。这些适配插座在结构上有较大不同，主要可在以下几个方面进行区分。

（1）触点的接触方式。根据 IC 卡在插入或退出时，按触点压触和脱离的方式区分主要有两种。一种是滑触式结构（Sliding），这种方式，插座上的触点处于固定位置，IC 卡在插入或退出时，滑过与之不相关的位置，并滑接在固定的位置上，它的特点是结构简单、价格低。缺点是对卡的触点位置磨损较大，寿命仅为 5 万～10 万次。另一种是着陆式结构（Landing），这种结构下，IC 卡在插入过程中，插座上的触点与 IC 卡同步运动，逐步下压，并稳定于最终位置。由于在触点对卡的着力过程中，卡与触点间没有相对位移，因而对卡表面的磨损小，触点寿命长，可达 30 万～100 万次插拔，但其价格较滑触式高。

（2）卡的进退形式。卡的进退（插入和退出）过程，也是人机的交互过程，根据不同的使用需要，对卡的进退形式要求也有较大不同。现行市场 IC 卡插座主要有推入-拉出结构和电动式入出卡控制结构。

推入-拉出结构是最常见的一种结构形式。而电动式入出卡结构，是一种全自动的运作方式，走卡平稳、可靠，但结构复杂，价格贵。为防止人为的不正当操作，有些 IC 卡座还设计了防拔卡装置。

（3）外形尺寸。有些应用对 IC 卡座的外结构尺寸有着严格的要求，部分卡座被设计成超薄的结构形式，高度为 5mm 左右。

（4）适用于特殊场合的 IC 卡插座。

在户外或湿度、振动强度大的场合，普通的 IC 卡座不能满足使用要求，此时，防水型或抗振动形式的 IC 卡插座便是一种好的选择，这些卡座采取了密封防水设计及机械加固

等方法,使得在环境较恶劣的条件下,使用 IC 卡成为可能。

2) 选择 IC 卡适配插座时的几个重要指标

在选用 IC 卡适配插座时,以下几个重要的指标是不容忽视的。

(1) 触点的位置和压力。

(2) 触点的电气性能。

(3) IC 卡座的插拔寿命。

(4) 对卡的磨损程度。

(5) 价格因素。

其中,对卡的磨损,不但要看对卡的电气接触面的磨损,还要考查对卡的其他位置的磨损。此外,使用场合要求也是选择的一个重要指标。

11.2 接触式读写器的接口和读写控制

1. 读写器对 IC 卡的电源供给

读写器实现对 IC 卡的供电,并满足不带电插拔的要求。若带电插拔 IC 卡,有可能会给 IC 卡带来损伤,甚至损坏 IC 卡。因此,在插拔前应先断开向 IC 卡供电的电源,并切断其逻辑连接,实现对 IC 卡的保护。

读写器中向 IC 卡供电的电路应是一个相对独立于读写器中的其他电路,并提供完善的过流保护措施的稳压电路,这是由于它是一个独立于 IC 卡的设备,当有卡插入时,读写器便开始向 IC 卡提供其所需的能量。如果插入的是一张电源与地击穿的坏卡,或者是一个金属片之类的物质,就会造成供电电路的短路现象,若读写器中无过流保护措施,就会造成读写器的损坏。即便有保护措施,若与 IC 读写器的其他部分共同使用一个保护电路,就会干扰读写器的正常工作。

2. 接触式读写器对卡的控制与读写

对 IC 卡的控制与读写是读写器中的核心操作部分,在图 11.1 中称为 IC 卡协议实现单元。

1) IC 卡的插入/退出识别

IC 卡的插入与退出是通过 IC 卡适配插座上的一个开关来识别的,如果卡已插入到正确位置,IC 卡适配插座就会给出一个开关接通的信号,而一旦卡离开这个位置,该信号就会立即发生反转。对于手动式 IC 卡适配插座来说,这一信号已经足够了。为了确保 IC 卡已准确地插到位置,插入的识别过程必须加入消颤处理,在读写器中,当接收到开关接通信号,而且在一定时间(假设 5ms)延迟后接通信号仍存在,就认为是真的接通了,否则认为是颤动。

读写器对 IC 卡各触点的控制是一个直接涉及是否能安全可靠地操作 IC 卡的过程。

2) IC 卡的读写

不同类型的 IC 卡,其读写方式或数据协议是不同的。ISO 7816 标准对异步型 IC 卡的读写协议作了较充分的定义,而对于同步型 IC 卡,则只定义了其复位响应过程的协议标准,这使得各厂家设计的同步型 IC 卡的读写方式不尽相同。而且由于同步型

IC 卡主要是不带微处理器的 IC 卡，接口协议是面向操作而进行的，因此，其操作协议也各不相同。

异步型 IC 卡大多带有微处理器，对卡的操作有 ATR 过程和 COS 命令的传递与响应过程。

IC 卡的通信字节格式是读写器能够准确与 IC 卡进行数据交换的基础，读写器必须在初始读入复位应答 ATR 时(即读入 TS 字节时)，便进入正确的状态判断。从复位应答过程的开始(TS 字节从 IC 卡中送出)到应答过程终止(TCK 字节送出)的时间应进行限制，过长的超时时间会影响系统的操作性能。

当读写器处理 ATR 正常结束后，将根据应用需求，并按 ISO 协议向卡发送命令，IC 卡处理后返回响应。卡内处理过程由 COS 和硬件实现。读写器在应用与卡之间起桥梁作用。

11.3 非接触式 IC 卡和 RFID 读写器的接口电路和读写控制

11.3.1 非接触式 IC 卡读写器的基本结构

非接触式 IC 卡应用系统一般由图 11.2 所示的三大部件组成：主控机、读写器和 IC 卡。

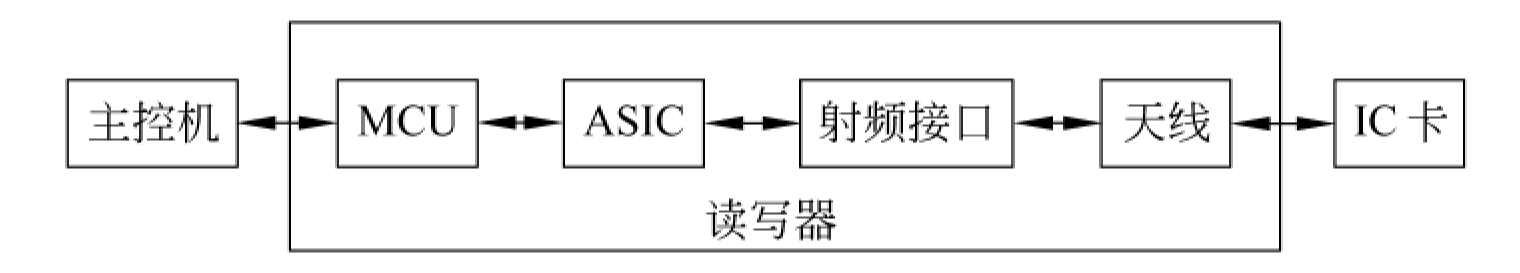


图 11.2 非接触式 IC 卡应用系统基本结构

主控机是应用系统控制管理中心，它可以是一台 PC，也可以是某信息管理系统的一个子集或前端，根据应用情况，可连至内部的局域网或外部的互联网、物联网。

读写器由四部分组成：MCU(微控制器)、ASIC(专用集成电路)、射频接口和天线。其中，MCU 和 ASIC 为数字电路，射频接口为模拟电路，天线用于传送能量和发送/接收射频信号。有关射频接口的工作原理参阅第 8 章。读写器工作范围内的多卡冲突处理见第 9 章和第 10 章。

MCU 和 ASIC 是读写器的控制单元。MCU 一般选用市场上广泛采用的普通微处理器。假如读写器尺寸或功能不受限制，或者专用集成电路 ASIC 的批量不大，可考虑用市场上供应的器件组成控制部件取代图 11.2 中的 ASIC。

MCU 和 ASIC 的功能如下。

(1) 以并行方式或串行方式(USB)与主控机通信，并执行主控机发来的命令。

(2) 通过高频接口与 IC 卡通信。

(3) 实现卡机之间通信数据的奇偶校验和(或)CRC 校验。即为拟发送给 IC 卡的数据生成奇偶校验位和(或)CRC 校验字节，并自动加在发送的字节和(或)帧之后；为接收到的 IC 卡信息进行奇偶校验和(或)CRC 校验，并自动去除奇偶校验位和(或)CRC 校验

字节，同时对校验结果进行处理。

(4) 编码和加密向 IC 卡发送的数据，解密和解码从 IC 卡来的数据。

(5) 进行多卡同时进入读写器射频场的防冲突处理。

(6) 实现卡机之间的相互鉴别。

MCU 接收主控机的命令，并发出具体操作命令，控制 ASIC 经由射频接口和天线实现对 IC 卡的所有操作。MCU 与 ASIC 之间的通信一般采用并行总线，而 ASIC 与射频接口之间的通信则采用串行方式，所以在读写器中还要实现并/串和串/并行数据的双向转换。

为了实现上述功能，在有微处理器的读写器中有操作系统，其复杂程度与主控机的分工有关。

鉴于非接触通信的复杂性和各厂家新产品在性能特点、遵循的协议和结构有大的差异。芯片制造商往往为其非接触式 IC 卡的读写器生产包含上述 ASIC 功能和(或)射频接口的专用读写芯片。下面将介绍 Philips 公司的 MFRC500 高集成度读写芯片。

11.3.2 MFRC500 高集成度读写芯片

1. 主要特性

MFRC500 是 Philips 公司于 21 世纪推出的 13.56MHz 的高集成度非接触读写芯片，支持 ISO/IEC 14443 Type A 协议，其发送部分可直接驱动天线，工作距离为 10cm，接收部分有解调和解码电路，数据处理部分有奇偶校验和 CRC 校验，支持快速 CRYPTO 1 流密码加密算法。其并行接口可直接与多种 8 位微处理器相接。其主要特性可归纳如下。

(1) 高集成度的调制解调电路。

(2) 输出缓冲驱动器通过少量外部无源器件连接天线，最大工作距离为 10cm。

(3) 支持 ISO/IEC 14443 Type A 协议。

(4) 采用 CRYPTO 1 加密算法和内部密钥 E^2PROM 存储器。

(5) 带内部地址锁存的并行微处理器接口和 IRQ 中断申请线。

(6) 可编程中断处理、定时器和初始化配置。

(7) 64B 的接收/发送 FIFO(先进先出)缓冲器。

(8) 64B 控制寄存器组，直接控制 MFRC 500 芯片的各种操作，并表示该芯片所处的状态。

(9) 数字、模拟和发送部分经独立引出端分别供电，且具备多种节电模式。

(10) 内部振荡缓冲器连接 13.56MHz 石英晶体振荡器。

(11) 面向位或字节的帧结构。

(12) 支持防冲突操作。

2. 功能框图

如图 11.3 所示，上半部为数字电路，下半部为射频接口。

MFRC500 芯片共有 32 个引出端，分成如下 3 种类型。

(1) 电源线与地线(7 根)。数字电路、模拟电路(射频接口)和发送射频的端口分别由 DVDD 和 DVSS、AVDD 和 AVSS 及 TVDD 和 TVSS 供电，其中 DVDD、AVDD 和

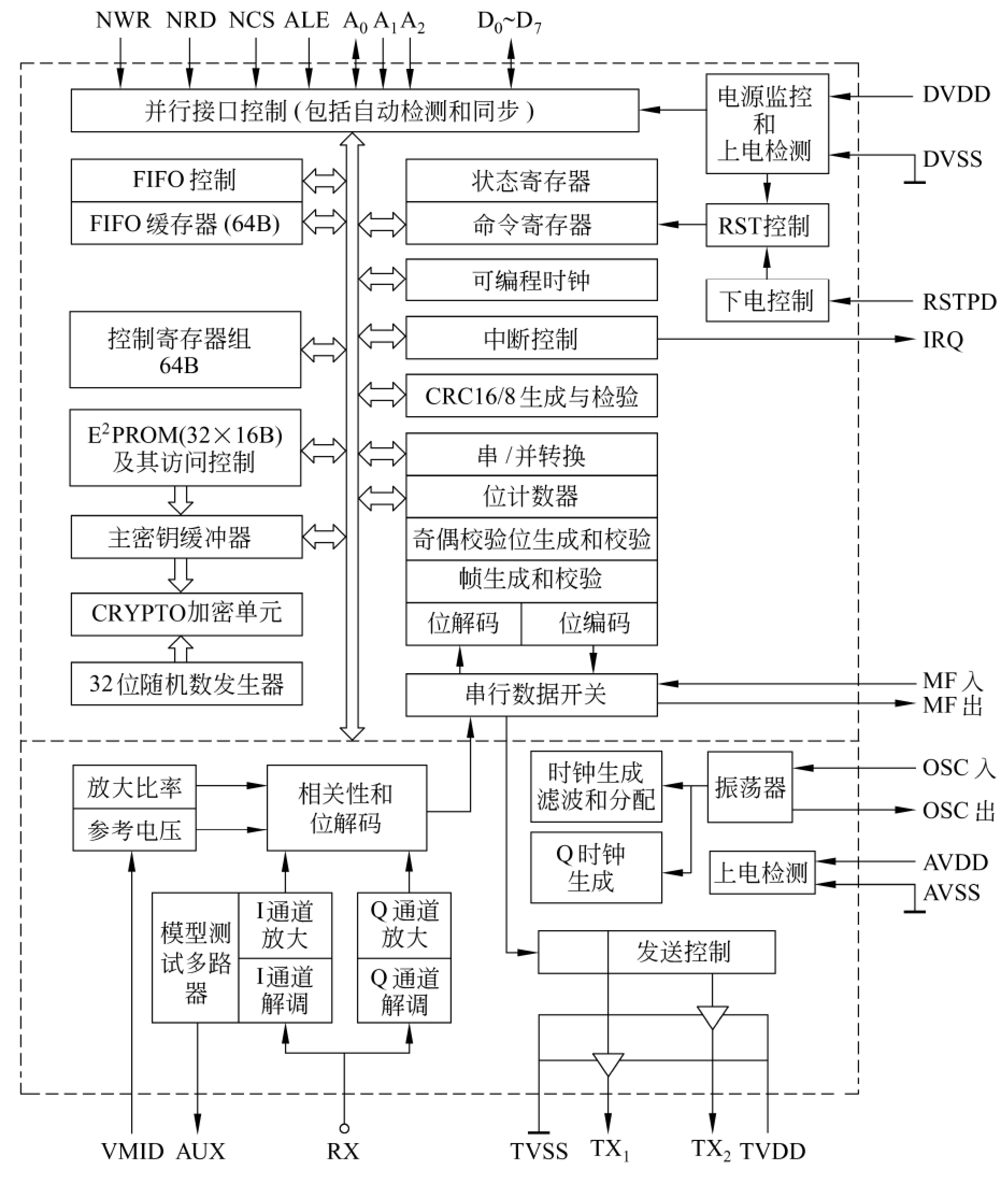


图 11.3　MFRC500 读写芯片功能框图

TVDD 为电源端，DVSS、AVSS 和 TVSS 在芯片外部接地。设置 3 对电源线和地线的目的是减少电源线和地线引起的相互干扰。

另外，还有一个放大器参考电压 VMID。

(2) 数字电路部分的引出端(19 个)。数字电路部分主要与读写器内部的微处理器连接，该芯片的并行接口可与多种不同类型的微处理器相接，其中部分连线的连接方法与微处理器有关。

① $D_0 \sim D_7$ 或 $AD_0 \sim AD_7$(I)。连接地址线与数据线分开的微处理器时为 $D_0 \sim D_7$，而对地址线与数据线复用的微处理器则为 $AD_0 \sim AD_7$。

注：括号内的 I 表示输入(IN)，O 表示输出(OUT)。

② $A_0 \sim A_2$(I)，寄存器地址线。对某些微处理器(带握手功能)，A_0 可作为 MFRC500

芯片输出的等待信号，A_0 为低电平表示一访问周期开始，高电平表示结束。

③ ALE(I)，地址锁存。AD_0～AD_5 锁存入内部地址锁存器。

④ NWR 和 NRD(I)，写选通与读选通。

MFRC500 与多种接口类型不同的微处理器相连时，连接方法有所区别。接口类型有：读/写选通共用且地址和数据总线独立或复用的接口；读/写选通分离且地址和数据总线独立或复用的接口；读/写选通共用且带握手通信功能的接口。

⑤ NCS(I)，芯片选择。微处理器选择和激活 MFRC500。

⑥ IRQ(O)，中断请求。有定时器中断、发送接收中断、FIFO 缓冲器空/满中断等。

⑦ RSTPD(I)，复位和掉电。

⑧ MF 入和 MF 出(I 和 O)。传送的串行数据流，符合 ISO/IEC 14443 Type A 协议。

(3) 射频接口引出端(6 个)。

① OSC 入和 OSC 出(I 和 O)，石英振荡器输入和输出。也可输入 13.56MHz 外部时钟。

② RX(I)，接收输入。接收 IC 卡响应信号负载调制的 13.56MHz 载波。

③ TX_1 和 TX_2(O)，发送输出。输出调制的 13.56MHz 载波。

④ AUX(O)，辅助输出。输出模拟测试信号。

3. 命令系统

命令是通过写命令代码到命令寄存器(Command Register)来启动，处理命令所需的参数和数据主要是通过 FIFO 缓存器交换的。MFRC500 命令的一般规则如下。

(1) 命令中需要输入的数据流直接来自 FIFO 缓存器。

(2) 命令中需要的参数数量，仅当从 FIFO 缓存器获得正确的数量时，才能启动命令的执行。

(3) 当命令启动时，FIFO 缓存器内容不清除。

(4) 每一条命令(Start Up 命令除外)都可被 MCU 写入命令寄存器的新命令所打断。

MFRC500 定义的命令系统如表 11.1 所示。

表 11.1　MFRC500 命令

命　令	作　　用
Start Up	由上电或硬件复位激活
Idle	中止当前执行命令
Transmit	将 FIFO 缓存器内容送卡
Receive	激活接收电路，在延迟时间之后，方可启动接收器
Transceive	将 FIFO 缓存器内容送卡，然后启动接收器，是 Transmit 和 Receive 命令的集合
Write E2	将 FIFO 缓存器中数据写入 E^2PROM
Read E2	将卡内 E^2PROM 数据读入 FIFO 缓存器(密钥区不可读)
Load Key E2	从 E^2PROM 复制一密钥至密钥缓存器

续表

命　令	作　　用
Load Key	从 FIFO 缓存器读一密钥至密钥缓存器
Authent 1	进行 CRYPTO 1 认证的第 1 步
Authent 2	进行 CRYPTO 1 认证的第 2 步
Load Config	从 E^2PROM 读数据并初始化控制寄存器
CalcCRC	计算 CRC 码

11.4　读写器的操作流程

读写器对接触式智能卡的控制程序如图 11.4 所示。

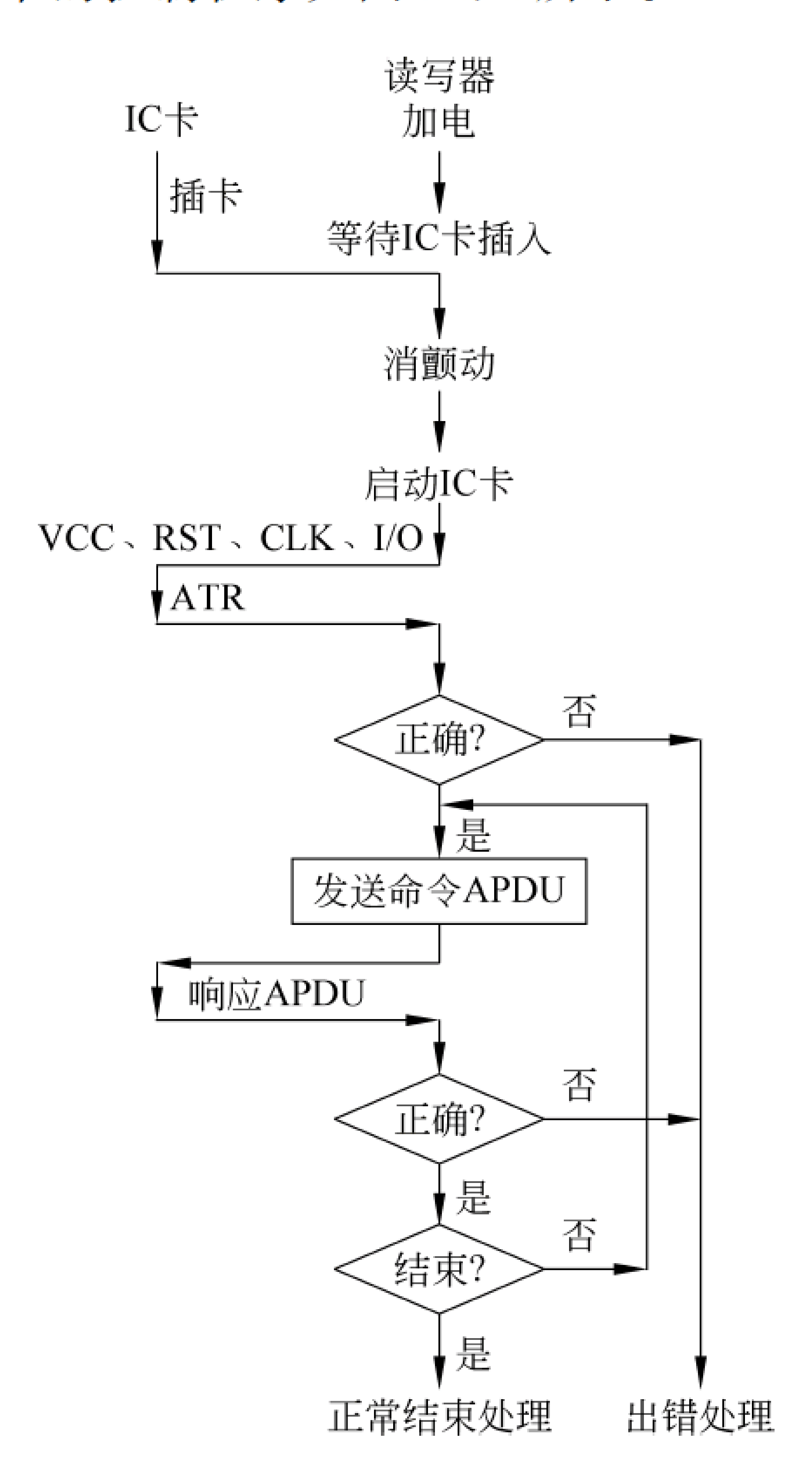


图 11.4　读写器的操作流程

从 IC 卡插入到接收 ATR 为止，全部由硬件完成，然后由读写器处理，如果没有问题，则由读写器发命令 APDU，IC 卡处理，返回响应 APDU，如果 SW1-SW2 为 9000，说明命令已正常处理，如果为其他值，则进行出错处理，根据 SW1-SW2 指出的出错情况进行具体处理，例如数据重发、持卡人重新输入密码等，甚至结束运行。在正常情况下，命令响应循环执行。

一般在读写器上都设置有可供操作人触摸的显示屏。

读写器的操作系统一般存放在 ROM 或 E^2PROM 中。

非接触式 IC 卡或射频标签要先进行防冲突仲裁，读出 UID(唯一标识符)。

11.5 射频识别读写器的种类和发展趋势

1. RFID 标签的读写器种类

在智能卡和 RFID 标签的应用领域中，最早使用的是接触式 IC 卡，由于非接触式 IC 卡要解决天线、射频识别、调制解调等问题，造成价格较高的局面，而且信号在空中传输，容易被他人截取，其安全性更要关注。目前非接触式 IC 卡已得到广泛应用。读写器与卡是同步发展的，本书有不少章节已对 IC 卡标准进行了论述，实际上也相当于对读写器的功能提出了要求。

RFID 标签应用范围较广，一般将非接触式 IC 卡包含在 RFID 标签范围内，RFID 读写器大致可分类如下。

(1) 固定式读写器。将射频控制器和射频接口封装在一个固定的外壳中，有时将天线也封装其中。供电电压：若为直流一般为 12V，交流为 220V/110V。工作温度有室内、室外之分。要注意环境温度，一般读写器的存储温度范围比工作环境广。

(2) OEM 读写器。将原始设备制造(Original Equipment Manufacture, OEM)读写器提供给用户。集成到用户终端或其他设备中。供电电压为 12V。

(3) 工业控制器。大多具备标准的现场总线接口，以备集成到工业设备中，主要应用在矿井、生产自动化等领域。根据环境的需求提供不同的防护功能，如防爆、防湿和防震等。

(4) 便携式读写器。这是适合于用户使用的一类电子标签读写设备，一般用于检查设备、付款往来、操作记录等，还带有输入数据和显示功能。

通常可以选用 USB 接口和 PC 之间实现数据传送，并有一定存储容量和内置天线。

(5) 发卡机。用来对电子标签进行具体内容的操作，包括建立档案、卡中充值、挂失、补发卡、修改密码和其他信息等。

2. 射频识别读写器的发展趋势

随着射频识别技术的发展和应用系统的扩展，对读写器提出了更高的要求，未来的高性能读写器将会有下述特点。

(1) 多功能和多样性。为了适应某些应用，读写器将具有更多智能性，具有一定的数据处理能力。如果用作互联网或物联网的基层设备，将获得应用系统的高度发展。

(2) 小型化、便携式、嵌入化。减小读写器的体积，便于携带和使用。降低功耗，在电池供电的情况下可延长使用时间。

(3) 多种数据接口。适应应用领域的扩展。可提供多种形式接口，如 USB、红外、无线局域网(WLAN)等。

(4) 多天线结构。如果具有多个天线，读写器可按一定的处理顺序打开和关闭不同

天线,使系统能感知不同天线覆盖区域内的电子标签或不同相位的电子标签。

(5) 多制式电子标签和多频段电子标签的适应性。

(6) 降低成本。

11.6 IC 卡和读写器的测试技术与标准

为了保证识别卡的可靠性和可用性,1993 年国际标准化组织制定了测试标准——《识别卡测试方法》(ISO/IEC 10373)。它规定了磁卡、IC 卡和光卡等识别卡一般特性的测试方法。后来又进行了修订。

测试应在温度为 23℃±3℃和相对湿度为 40%~60%的环境下进行。要求预处理,在测试前应将待测试的卡在上述测试环境中放置 24h。

测试设备的特性和测试方法规程给出的量值默认容差为±5%。

另外,在 IC 卡和标签的整个生命周期内要经历设计与制造、初始化等多个阶段,在每个阶段都应满足功能与安全的要求。尤其在设计与制造阶段要通过多个部门的合作、多个步骤的实现才能完成任务,而且每一步操作都可能产生废品,因此几乎在每一工序后都要进行详细测试;否则,可能会给最后的成品带来极大危害。

当 IC 卡和标签制造出来以后,从安全出发,外部对其进行的任何操作都是通过 COS(卡内操作系统)实现的,因此无论是在设计阶段还是设计完成后,对 COS 的测试都是极为重要的。在第 7 章通过一个小型 COS 的例子来说明如何进行测试。

11.6.1 IC 卡的机械和物理特征的测试

1. 一般性的测试

在国际标准 ISO/IEC 10373-1 中主要描述了 IC 卡一般特性的测试内容方法和指标。

根据卡的不同特性,规定了可选择的测试项目,内容包括卡的翘曲(扭曲和弯曲)、卡的尺寸(长、宽、厚度)、剥离强度、卡片之间的粘连、可燃性、紫外线、X 射线、电磁场、抗热度等。

2. 接触式 IC 卡物理特性

1) 接触式 IC 卡物理特性测试方法

(1) 触点的尺寸和位置。测试每个触点是否符合 ISO/IEC 7816-2 规定的区域,并检查该区域是否完全由触点的金属表面覆盖,以及该触点保证不与其他的触点相连。

(2) 静电。测试静电电位对 IC 卡的影响。根据实际应用,选择 IC 卡能承受的电压限值。

(3) 触点的表面电阻。将两个测试探针加到 IC 卡触点上,测量加在两个触点上的测试探针之间的电阻,可设定触点表面的最大允许电阻为 500mΩ。

(4) 触点表面轮廓。测量 IC 卡触点和 IC 卡表面之间的厚度差别,向上不超过

0.05mm，向下不超过0.1mm。

（5）机械强度。卡应能在一定范围内抵抗对其表面及其任何组成部件的损害，并在正常使用、保存和处理过程中保持完好。

2）读写器的位置

读写器应保证IC卡插拔顺利可靠，与IC卡触点接触位置正确、压力适当。

3）测试设备

为了测试IC卡的电气特性和逻辑操作功能，需要一台能仿真读写器的装置（即IC卡的测试设备），这台设备能对IC卡的全部功能及出错处理程序进行全面测试，并对各触点能提供比正常操作时更宽的电压和电流变化范围及时序信号，并能运行测试程序。

同样，为了测试读写器的电气特性和逻辑操作功能，需要一台能仿真IC卡的测试设备，这台设备测试读写器能否实现对IC卡各触点的电流和电压的要求，并有仿真异步卡协议或同步卡协议运行的测试程序。

11.6.2 异步卡（接触式IC卡）和读写器的电气特性测试

1. 接触式IC卡

（1）VCC触点。测量卡在VCC触点上所消耗的电流，并检测在给定的V_{CC}范围内（(1±5%)V_{CC}）IC卡能否正常工作。

（2）I/O触点。测量I/O触点的接触电容。测量IC卡发送数据时在正常工作模式下I/O触点的输出电压，以及I/O触点上波形的上升沿t_R和下降沿t_F；接收数据时I/O端的输入电流。

（3）CLK触点。在卡支持的电压下，测量IC卡CLK触点的电流，检测IC卡在一给定时钟频率和波形下能否运行。

（4）RST触点。测量卡在RST触点上所消耗的电流，并检测RST信号在允许的最小和最大时间值范围内和给定的电压值下IC卡能否正常工作。

2. 读写器电气特性

（1）触点激活顺序。测量IC卡激活时读写器提供给各触点的电压或信号顺序。

（2）VCC触点。测量由读写器给VCC触点提供的电压。

（3）I/O触点。测量I/O触点的接触电容；测量在正常工作条件下I/O触点输出电压；测量在读写器发送模式下I/O触点的上升沿t_R和下降沿t_F，以及接收模式下I/O触点的输入电流。

（4）CLK触点。测量CLK信号的特性。测量在ATR期间CLK触点上的电压、t_R、t_F和占空比。

（5）RST触点。测量RST信号的特性。

（6）暂停。测量读写器暂停时序。记录所有读写器触点信号的电平和时序。

11.6.3 接触式 IC 卡和读写器的逻辑操作测试

1. IC 卡的逻辑操作测试

本节根据 ISO/IEC 7816-3 标准测试 IC 卡的逻辑操作特性，测试仪器应能产生 IC 卡所需的测试信号。并记录下被测信号的电平、时序和内容。

1）复位应答

测试 IC 卡在复位期间的性能。首先激活 IC 卡，在 CLK 激活后，测试仪器在 400 个时钟周期后将 RST 设为高。如果 IC 卡返回复位应答信号，则从 ATR 中至少选择一个字符（随机选择）作为传输错误。然后，IC 卡运行一段测试程序，测试并分析复位期间 IC 卡发送数据的电平、时序和内容。

如果 IC 卡不能发出 ATR，则停止测试。

2）传输协议（$T=0$）

（1）$T=0$ 协议的 I/O 发送时序。测试 IC 卡数据发送的时序。IC 卡以正常的位时序参数运行一段测试程序，在 PPS 的控制下，改变 ETU 因子（通过改变 F 和 D）。

（2）$T=0$ 协议的 I/O 字符重发。测试 IC 卡的字符重发的时序和用法。IC 卡以正常的位时序参数运行一段测试程序，IC 卡发送一个字节，产生一个错误的奇偶校验位。

（3）$T=0$ 协议下，I/O 接收时序和出错信号。测试 IC 卡的接收时序和出错信号。IC 卡运行一段测试程序，在一个字节的有效位发送完成后，发送错误的奇偶校验位。

3）传输协议（$T=1$）

（1）$T=1$ 协议下 I/O 发送时序。测试 IC 卡数据发送的时序。IC 卡运行一段至少 1s 时间的 $T=1$ 协议的应用程序。在 PPS 的控制下，每提供一个 ETU 因子，重复上述过程。

（2）$T=1$ 协议下 I/O 接收时序。测试 IC 卡在 $T=1$ 协议下数据接收的时序。IC 卡运行一段至少 1s 时间的 $T=1$ 协议的应用程序。

（3）IC 卡字符等待时间特性。

① 字符等待时间（两个相邻字符上升沿之间的最大时间）。向 IC 卡发送具有 n 个字节的数据块，记录 IC 卡响应是否存在及响应的内容和时序。

② IC 卡对读写器超过字符等待时间的反应。测试当读写器超过字符等待时间时，IC 卡的反应。记录 IC 卡响应是否存在及响应的内容和时序。

（4）块保护时间。测试在相反方向上所发送的两个块的字符前沿之间的时间。

（5）IC 卡的块传输差错的反应。发送一个错误块给 IC 卡。错误块中有一个或多个奇偶校验错误或块的结尾有错误的 EDC（LRC 或 CRC）。考虑是否重发。

（6）IC 卡对协议传输差错的反应。测试仪器发送一个错误块给 IC 卡。错误块可以是一个无效块，它带有未定义的 PCB 编码，或者 IC 卡发回与 PCB 期望不匹配的信息。

（7）读写器放弃。测试卡是否支持由读写器所要求的放弃。

2. 读写器逻辑操作测试

1）复位应答

IC 卡的复位和复位应答。激活读写器；持续监视复位信号至少 1s，并测试时序（与时

钟信号相关)和在各触点上的时序和电平变化。

2) $T=0$ 协议

(1) $T=0$ 协议,I/O 传输时序。测试读写器数据传输时序。

(2) $T=0$ 协议,I/O 字符重发。测试读写器重发字符的使用和时序。

(3) $T=0$ 协议,I/O 接收时序和错误信号。测试读写器接收时序和错误信号的处理。

3) $T=1$ 协议

(1) $T=1$ 协议,I/O 发送时序。测试读写器数据发送时序。

(2) $T=1$ 协议,I/O 接收时序。测试使用 $T=1$ 协议时的读写器数据接收时序。

(3) 读写器字符等待时间特性。测试读写器对 IC 卡超过字符等待时间的反应。

(4) 块保护时间。测试反向发送的两字符前沿之间的时间。

(5) 读写器对传送错误的恢复。测试读写器对"否定确认"的处理。

读写器逻辑操作的测试方法与 IC 卡逻辑操作的测试方法雷同,因此,对本节中的内容不再说明。

11.6.4 非接触式卡测试方法

非接触式 IC 卡和接触式 IC 卡的基本差别如下。

(1) 卡上无触点,从天线上接收信息与发送信息。

(2) 卡内电路所需的直流电压,一般将天线上接收的载波信号整流后形成。

(3) 在读写器的工作范围内可能存在多张 IC 卡,因此需要解决卡之间的冲突问题,即防冲突。

(4) 在读写器和 IC 卡中,需要测试如何将数字信号转换成射频信号(调制),以及将射频信号转换成数字信号(解调)。

目前存在多种射频技术(见第 8 章),IC 卡选择一种方案实现信号和数据的传送需要进行实验与测试。同时也需要测量直流电压值,能否正常提供给卡内数字电路、微控制器和存储器使用。

在本书第 9 章和第 10 章介绍的多个非接触式 IC 卡和 RFID 标签用的空中接口国际标准中定义了不同的射频信号表示方式和防冲突协议的实施方案等,其性能需要在 IC 卡的设计、实验和芯片生产阶段(芯片封装前)进行测试,因为芯片的成品不具有可供测试的触点。

IC 卡测试:对该卡根据空中接口国际标准制订的方案和卡内使用的每条命令进行功能测试和可靠性测试,实现防冲突和信号、数据的传输功能。最后对 IC 卡的应用程序进行测试,验证卡内的硬件和操作系统(COS)的正确性。

目前 ISO/IEC 还没有制定完整实施非接触式 IC 卡的应用命令和与安全性有关的命令等,建议还可采用 ISO/IEC 7816 中定义的命令。

在测试中还需对天线上信号进行测试;在读写器产生的磁场强度范围内($H=5\sim150\text{mA/m}$)卡的正常工作能力;读写器与 IC 卡之间的工作距离等。

11.7 智能卡复位应答(ATR)和命令系统的测试

1. ATR 的测试

在仿真读写器中预存 ATR,并与卡返回的 ATR 比较,如果相等,则进行命令系统的测试。

2. 各条命令的测试

(1) 智能卡中各条命令的功能是由卡内操作系统(COS)控制的硬件完成的,对卡的试制品和市场上的成品测试方法一般是不同的,前者需对卡进行全面测试,并能迅速找出出现问题的原因,甚至对硬件的组成部件进行测试,这与产品的质量和应用场合有关。

(2) 测试设备。由计算机控制下的读写器或仿真读写器发出测试卡的命令,并将卡返回的响应数据(如有的话)和 SW1-SW2 提交给计算机或仿真读写器进行分析,甚至可能出现测试程序中断或其他异常情况。

(3) 各命令测试顺序的安排。功能较简单或测试其他命令需要提前执行的命令在时间上安排在前面测试,计算机可为测试提供改变顺序的功能。

3. IC 卡命令的测试举例(命令来自第 6 章)

1) UPDATE BINARY(更新二进制)命令的测试

本测试证实该命令在功能、性能和安全性等方面是否符合相关国际标准和产品的设计目标,如有不符,则须改正。通过本例,希望读者能初步了解在测试时读写器怎样发命令,以及如何从卡返回的响应来检验命令执行的正确性,并增加对卡内各条命令的先后测试次序如何安排的认识。

在本例中,假设在测试前已用 CREATE FILE(创建文件)命令创建了两个 EF 文件,标识符为'0001'和'0002'。

测试后,卡返回 SW1-SW2,参见表 6.4 和表 6.5。

(1) 功能正确情况测试。

测试目的:验证卡片是否正确执行该命令,并正确响应。

测试原理:在输入的参数都合法、执行的条件都具备的情况下,安排测试程序,检查所测命令是否能够正确执行。

实例如表 11.2 所示。

在表 11.2 中安排了 3 条命令,首先将当前文件设置为'0001',如果此前已是'0001',则可以不安排,其后安排的 READ BINARY 命令是为了检验更新的数据是否正确。此例说明在测试 UPDATE BINARY 命令之前,应先测试另外两条命令。从测试总体考虑,还应该先测试 WRITE BINARY 命令。

表 11.2 功能正常情况测试

测 试 项 目	UPDATE BINARY 命令的功能正确情况测试
测试内容描述	测试 UPDATE BINARY 命令执行后相应数据是否成功写入文件
参考文档	ISO/IEC 7816-4

测 试 项 目	UPDATE BINARY 命令的功能正确情况测试
测试初始条件状态	建立二进制文件'0001'并满足执行命令的安全属性
测试程序	(1) 选择该二进制文件,执行 SELECT 命令,当前文件标识符为'0001' (2) 执行 UPDATE BINARY 命令(CLA='00',INS='D6',P1='00',P2='00',Lc='10',数据域为 16B 随机数 Random) 卡片返回'9000' (3) 执行 READ BINARY 命令(CLA='00',INS='B0',P1='00',P2='00',Le='10') 卡返回的数据等于 16B 随机数 Random,SW1-SW2 为'9000'

(2) 功能异常情况测试。

测试目的:验证卡片的每条命令是否对异常情况可以正确执行,并返回相应错误代码。

测试原理:输入的参数都合法,但执行的条件不具备,检测卡是否返回了相应错误代码。

实例如表 11.3 所示。

表 11.3 功能异常情况测试

测 试 项 目	UPDATE BINARY 命令更新的文件不是二进制文件
测试内容描述	UPDATE BINARY 命令更新的文件不是二进制文件,在 IC 卡的响应中是否能返回期望的错误代码
参考文档	ISO/IEC 7816-4
测试初始条件状态	建立二进制文件'0001',建立记录文件'0002',并满足执行命令的安全属性
测试程序	(1) 选择一个记录文件'0002'(执行 SELECT 命令,当前文件为'0002') (2) 执行 UPDATE BINARY 命令(CLA='00',INS='D6',P1='00',P2='00',Lc='10',数据域为随机数 Random) 卡返回错误代码,SW1-SW2 为'6981'

2) 命令类别(CLA)测试

测试目的:验证每条命令存在错误 CLA 时是否可以返回期望的错误代码。

测试原理:固定所测命令参数 P1、P2、Lc 和数据域正确且不变的情况下,利用穷举法遍历每一个错误的 CLA 作为输入,测试卡是否返回了相应的错误代码。

CLA=00 时,正确,其他值'01'~FF 为错误,其根据是:

假设 CLA 类别符合表 11.2 中的定义,又卡中不存在 GET RESPONSE 命令,因此无命令链存在,且仅传输明文数据,使用基本逻辑通道。

实例如表 11.4 所示。

表 11.4　CLA 测试

测 试 项 目	UPDATE BINARY 命令的 CLA 参数测试
测试内容描述	测试当 UPDATE BINARY 命令的 CLA 错误时,COS 是否可以不执行该命令,并返回期望的错误代码
参考文档	ISO/IEC 7816-4
测试初始条件状态	建立二进制文件'0001'并满足执行命令的安全属性
测试程序	(1) 选择该二进制文件(执行 SELECT 命令),当前文件标识符为'0001' (2) 执行 UPDATE BINARY 命令时 CLA 送入'01'～'FF'中的一个,卡返回 SW1-SW2 为'6E00'

3) 安全机制测试

测试目的:验证卡片在不满足安全状态的情况下是否可以拒绝操作。

测试原理:在操作一个基本文件时,该文件可能有一个或多个安全控制机制。在其中一种安全控制机制不满足的情况下,COS 是否能正确检查出来。当多种安全控制机制不满足的情况下,COS 是否能正确检查出来。

实例如表 11.5 所示。

表 11.5　安全机制测试

测 试 项 目	UPDATE BINARY 命令更新文件时,安全条件不满足该二进制文件的安全属性
测试内容描述	UPDATE BINARY 命令更新文件时不满足该二进制文件的安全属性,COS 是否能中止命令的执行并返回期望的错误代码
参考文档	ISO/IEC 7816-4
测试初始条件状态	建立二进制文件'0001'并不满足安全属性
测试程序	(1) 选择该二进制文件(执行 SELECT 命令) (2) 执行 UPDATE BINARY 命令(CLA='00',INS='D6',P1='00',P2='00',Lc='10',数据域随机数 Random) 卡片返回 '6982' (3) 执行相应的认证程序,使安全状态满足安全属性的要求 (4) 执行 UPDATE BINARY 命令(CLA='00',INS='D6',P1='00',P2='00',Lc='10') 卡片返回数据为随机数 Random,SW1-SW2 为'9000'

4) 防拔测试

测试目的:验证卡片在执行带有写操作的命令突然断电时,COS 能够成功保护数据的功能。

测试原理:当卡片在进行写 E^2PPROM 操作的时候如果突然断电,卡片只能有两种选择:一是写操作全部完成,新数据成功写入;二是写操作全部未执行,E^2PROM 中的数据应完整保存原有数据。其他任何情况都视为错误。

实例如表 11.6 所示。

表 11.6　防拔测试

测 试 项 目	UPDATE BINARY 命令防拔测试
测试内容描述	执行 UPDATE BINARY 命令更新文件时断电,COS 应能成功保护数据
参考文档	ISO/IEC 7816-4
测试初始条件状态	建立二进制文件'0001'
测试程序	(1) 选择该二进制文件 执行 UPDATE BINARY 命令(CLA＝'00',INS＝'D6',P1＝'00',P2＝'00',Lc＝'10',数据域为 16B 随机数 Random1) 卡片返回 '9000' (2) 写入 Random2 ① 选择该二进制文件 ② 执行 UPDATE BINARY 命令(CLA＝'00',INS＝'D6',P1＝'00',P2＝'00',Lc＝'10',数据域为 Random2) ③ 令读写器发出命令 APDU 之后 1～500ms 使 IC 卡断电 (3) 防拔结果检查阶段 ① IC 卡加电,复位卡片 ② 选择该二进制文件 ③ 执行 READ BINARY 命令(CLA＝'00',INS＝'B0',P1＝'00',P2＝'00',Le＝'10') ④ 卡片返回数据和 SW1-SW2('9000') 数据等于 Random1 或 Random2。数据如果不等于 Random1 也不等于 Random2 则报错,SW1-SW2 为'6A80' 返回数据可以等于 Random1 也可以等于 Random2,读写器接收数据后需进一步处理

习题

1. 从结构上划分,读写器可分成哪两种类型?叙述各种类型的主要组成部分。
2. 常用的读写设备的 IC 卡座有哪几种?
3. IC 卡的电源是由哪个设备提供的?在 IC 卡插拔过程中,在什么时候加上电压比较安全?与电源有关的保护措施有哪些?
4. 读写器中的微处理器起什么作用?它通过什么途径向 IC 卡(接触式和非接触式)或 RFID 标签发命令?
5. 非接触式 IC 卡读写器中专用的读写芯片,MFRC500 包括哪些功能部件?其中控制寄存器与 FIFO 缓存器的主要功能是什么?MCU 通过什么手段控制该芯片?
6. 请论述读写器和卡(或标签)之间的工作关系。
7. 试画出电话预收费卡读写器的工作流程。
8. 当采用异步传输协议时,应遵循的国际标准是什么?
9. 在持卡人的一次消费过程中,IC 卡与读写器是如何配合工作的?
10. 测试 ATR 的目的是什么?
11. 对测试设备的基本要求是什么?

12. 接触式 IC 卡有哪些电气特性测试和逻辑操作测试内容？
13. 同步卡和异步卡测试的主要差别是什么？
14. 非接触式 IC 卡与接触式 IC 卡的测试方法和内容有哪些是共同的？有哪些是不同的？
15. 卡(硬件和 COS)测试的重要性是什么？测试原则是什么？
16. 你认为要进行哪些测试才能认为卡是完好的，可以放心使用？如果发现存在错误，应该(或可能)采取怎样的补救措施？

第 12 章　物联网的体系结构与国家规划(设想、创新)

12.1　物联网的体系结构

1. 物联网定义

物联网(IoT),译自英文 the Internet of Things,由此可理解"物联网就是物物相连的互联网"。物联网的核心和基础仍然是互联网,是指通过各种信息传感设备,如传感器、射频识别(RFID)标签、全球卫星定位系统(GPS)、红外感应器、激光扫描器等各种装置,实时采集需要监控、连接、移动的物体位置或活动,采集其声、光、热、电或位置等信息,与互联网结合而形成的一个网络。其目的是实现物与物、物与人,所有的物品与网络的连接,方便识别、定位、跟踪、管理和控制。物联网本身具有智能处理的能力,从传感器获得的海量信息中分析、加工和处理出有意义的数据,以适应不同用户的不同需求,扩大应用领域。

物联网可让无处不在的终端设备通过各种无线/有线的长距离/短距离通信网络实现互联互通,提供安全可控乃至个性化的实时在线监测、定位追溯、报警联动、调度指挥、远程控制、安全防范、决策支持等管理和服务功能。

1999 年在美国召开的移动计算和网络国际会议上提出物联网概念:在计算机互联网的基础上,利用 RFID 技术、无线数据通信技术和 EPC(电子产品代码)标准等,构造一个实现全球物品信息实时共享的物联网。2005 年国际电信联盟(ITU)报告中,对物联网的定义和范围又发生了变化,覆盖范围有了较大的拓展,不再只是指基于 RFID 技术的物联网。

目前,物联网还没有公认的定义。由于物联网与领先发展、广泛应用的互联网、移动通信网、传感网等有密切关系,而不同领域的研究单位和生产单位对物联网有不同的认识。因此物联网的研发和应用还脱离不了相关领域。

2. 物联网体系结构

一般将物联网分成 3 个层次:感知层、网络层和应用层。

(1) 感知层。利用条形码标签和识读器、RFID 标签和读写器、摄像头、传感器(温度、湿度、声音、震动、压力感应器等)、全球卫星定位系统(Global Positioning System, GPS)等识别控制物体,采集数据信息。

(2) 网络层。利用移动通信系统、互联网、传统电信网等将感知层采集的信息进行处理和传递。

(3) 应用层。将网络层传送来的信息进行处理,做出控制和决策,实现信息的存储、数据的挖掘和应用的实施。从而实现智能化的管理、应用和服务。

物联网面向的民用对象可以是工业、商业、金融、农业、交通、电力、医疗、家庭和个人等。一般在网络层和应用层之间设置一个公用平台,以便于应用层的开发、移植和互

操作。

在我国自主控制的中文互联网平台有以百度为代表的信息服务(搜索)平台、阿里巴巴为代表的互联网金融(电商)平台、以腾讯为代表的社交(微信)平台。

目前,百度、阿里巴巴、腾讯虽然仍处于上述领域的霸主地位,但在业务方面,它们已处于相互渗透、竞争和发展的局面,并设立了若干个子公司,或合并、投资其他公司,增强了人与物、物与物的关联,提高了服务水平。

12.2 条形码

1. 一维条形码

传统条形码(也称一维条形码)技术相对成熟,在社会生活中处处可见,在全世界得到了极为广泛的应用。它作为计算机数据采集手段,以快速、准确、成本低廉等诸多优点迅速进入商品流通、自动控制及档案管理等各种领域,也是目前我国使用最多的一种条形码。

传统条形码由一组按一定编码规则排列的条、空元素组成,表示一定的字符、数字及符号信息。在条形码符号中,反射率较低的元素(黑条)称为条,反射率较高的元素(白条)称为空(图 12.1(a))。条形码系统是由条形码符号设计、条形码制作及扫描阅读组成的自动识别系统。

到目前为止,常见的条形码的码制大概有 20 多种,其中广泛使用的码制包括 EAN 码、Code39 码、交叉 25 码、UPC 码、ISBN 码及 CODABAR 码等。不同的码制具有不同的特点,适用于特定的应用领域,下面介绍一些典型的码制。

1) UPC 码(统一商品条码)

UPC 码在 1973 年由美国超市工会推行,是世界上第一套商用的条形码系统,主要应用在美国和加拿大。UPC 只提供数字编码,限制位数(12 位和 7 位),需要附加校验码,允许双向扫描(从左向右扫描和从右向左扫描),主要应用于超市与百货业。

2) EAN 码(欧洲商品条码)

1977 年,欧洲 12 个工业国家在比利时签署草案,成立了国际商品条码协会,参考 UPC 码制定了与之兼容的 EAN 码。EAN 码仅有数字号码,通常为 13 位,允许双向扫描,缩短码为 8 位码,也主要应用于超市和百货业。

3) ITF25 码(交叉 25 码)

ITF25 码的条码长度没有限定,但是其数字必须为偶数位,允许双向扫描。ITF25 码在物流管理中应用较多,主要用于包装、运输、国际航空系统的机票顺序编号、汽车业及零售业。

4) Code39 码

在 Code39 码的 9 个码素中,一定有 3 个码素是粗线,所以 Code39 码又被称为“三九码”。除数字 0~9,Code39 码还提供英文字母 A~Z 及特殊的符号,它允许双向扫描,支持 44 组条码,主要应用于工业产品、商业资料和图书馆等场所。

5) CODABAR 码(库德巴码)

CODABAR 码制可以支持数字、特殊符号及 4 个英文字母,由于条码自身有检测的

功能，因此无须校验码。主要应用在工厂库存管理、血库管理、图书馆借阅书籍及照片冲洗业。

6）ISBN码（国际标准书号）

ISBN是因图书出版、管理的需要，以及便于国际出版物的交流与统计，而出现的一套国际统一的编码制度。每一个ISBN码原由10位数字组成，在2007年增至13位，在前面加上3位(978)。用以识别出版物所属国别地区、出版机构、书名、版本及装订方式。这组号码也可以说是图书的代表号码，大部分应用于出版社图书管理系统。

条形码技术给人们的工作、生活带来的巨大变化是有目共睹的。然而，由于一维条形码的信息容量比较小，如商品上的条码仅能容纳几位或几十位阿拉伯数字或字母，因此一维条形码仅仅标识商品，而不包含对于相关商品的描述。只有在数据库的辅助下，人们才能通过条形码得到相关商品的描述。所以在没有数据库支持或联网不方便的地方，其使用就受到了相当大的限制。

另外，一维条形码无法表示汉字或图像信息。因此，在一些需要应用汉字和图像的场合，一维条形码就显得很不方便。现实的应用需要一种新的码制，这种码制除了具备一维条形码的优点外，还应该具备信息容量大、可靠性高、保密防伪性强等优点。

条形码可简称为条码。

2. 二维码

20世纪70年代，在计算机自动识别领域出现了二维码技术，这是在传统条形码基础上发展起来的一种编码技术，它将条形码的信息空间从线性的一维扩展到平面的二维，具有信息容量大、成本低、准确性高、编码方式灵活和保密性强等诸多优点。因此自1990年起，二维码技术在世界上开始得到广泛的应用。

与一维条形码只能从水平方向读取数据不同，二维码可以从水平、垂直两个方向获取信息，因此，其包含的信息量远远大于一维条形码，并且还具备自纠错功能。阅读二维码符号所包含的信息需要一个扫描装置和译码装置，统称为识读器。扫描器又称光电读入器，它装有照亮被读码的光源和光电检测器件，并且能够接收码的反射光，当扫描器所发出的光照在纸带上，根据纸带二维空间上各点信息的有无输出不同的图案，经放大、量化后送译码器处理。

二维码具有以下几个特点。

(1) 存储量大。

(2) 抗损性强。二维码采用故障纠正的技术，遭受污染及破损后也能复原数据。

(3) 安全性高。在二维码中采用了加密技术，所以使安全性大幅度提高。

(4) 可传真和影印。

(5) 印刷多样性。不仅可以进行彩色印刷，还可以直接印刷在被扫描的物品上或打印在标签上。

(6) 抗干扰能力强。具有强抗磁力、抗静电能力。

二维条形码分为以下两种类型。

(1) 线性堆叠式二维码。就是在一维条形码的基础上，降低条形码行的高度，将多个一维条形码在纵向堆叠而成，如图12.1(b)所示。目前已很少使用。

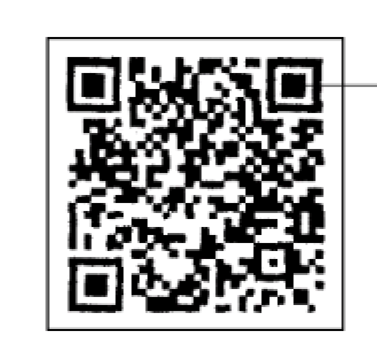
(2) 矩阵式二维码。如图 12.1(c)所示,采用统一的黑白方块(像素)的组合,是在计算机图像处理技术、组合编码原理基础上的图形符号自动识读处理的码制。它能够提供更高的信息密度,存储更多的信息。矩阵式符号没有标识起始和终止的模块,但它们有一些特殊的"定位符",如图 12.1(c)中有 3 个定位符,其中包含了二维码图形的定位、符号的大小和方位等信息。扫描后的图形有自动旋转到正确方位的能力。矩阵式二维码和新的堆叠式二维条形码能够用先进的数学算法将数据从损坏中恢复。



(a) 一维条形码



(b) 二维码(线性堆叠式)



(c) 二维码(矩阵式)

图 12.1　条形码示意图

12.3　RFID 标签的外形和系统架构

与 RFID 标签相关的射频识别技术和空中接口国际标准已在第 8～10 章详细论述,这是重点。在此对标签的封装和射频识别系统结构(举例)作简要介绍。

1. 电子标签的形状和封装

1) 电子标签的形状

根据应用场合而封装成不同的形状。

(1) 信用卡标签。其大小等同于信用卡,厚度不超过 3mm。

(2) 线形标签。常见的有流线形标签和车辆用线形标签,后者主要用于加强车辆在高速行驶中的识别能力和识别距离,用铆钉等将它固定在卡车的车架上或集装箱上。

(3) 盘形标签。盘形标签是最常见的一种电子标签,直径从几 mm 到 10cm,封装在塑料外壳内。

(4) 钥匙扣形标签。封装成钥匙形状外壳的电子标签,主要用于门禁系统。

(5) 自粘标签。是一种薄膜形标签,将标签安装在只有 0.1mm 厚的塑料膜上。这种薄膜往往与一层纸胶粘在一起,并在背后涂上胶黏剂,可以方便地粘贴在需识别的物品上。

(6) 其他标签。还有手表形标签及直接将天线制作在绝缘硅芯片上的微型标签等。

2) 电子标签的封装材料

为了保护标签的芯片和天线,以及以后使用方便,必须用某种材料进行封装。

(1) 纸标签。有自粘能力,可贴在被识别物品上的标签。其价格较便宜,一般由面层、芯片线路层、胶层和底层组成。面层一般由纸构成,允许印刷一些信息;芯片线路层与胶层黏合在一起;胶层起固定芯片和天线的作用,底层是标签使用前的保护层,使用时将底层撕下,即可将标签粘贴在被识别物的表面上。电子标签的成品可以是单张的,也可以是连续的纸卷。目前超市中的低价小物品,还难以用标签取代条码。

(2) 塑料标签。采用特定工艺将芯片和天线封装在塑料材质中的标签,一般由面层、

芯片层和底层组成，机械强度大。可用作钥匙牌、手表形标签、狗牌和信用卡等。

（3）玻璃标签。一般将芯片和天线用一种特殊的固定物质（软胶粘剂等）植入到只有12～32mm长的小玻璃管里，封装成玻璃标签。管内还装有稳定电压用的电容，天线的线圈是用0.3mm的线材绕在铁氧体磁芯上形成的。玻璃标签通常被用于动物跟踪与识别，可用注射器或其他方式植入到动物的皮下。

2. RFID系统结构（举例）

图12.2所示为一个典型的RFID系统各部分的关系及所涉及的标准化的内容。包括读写器与射频标签，读写器与应用系统之间的接口关系图，涉及通信协议、数据协议和一致性测试标准。

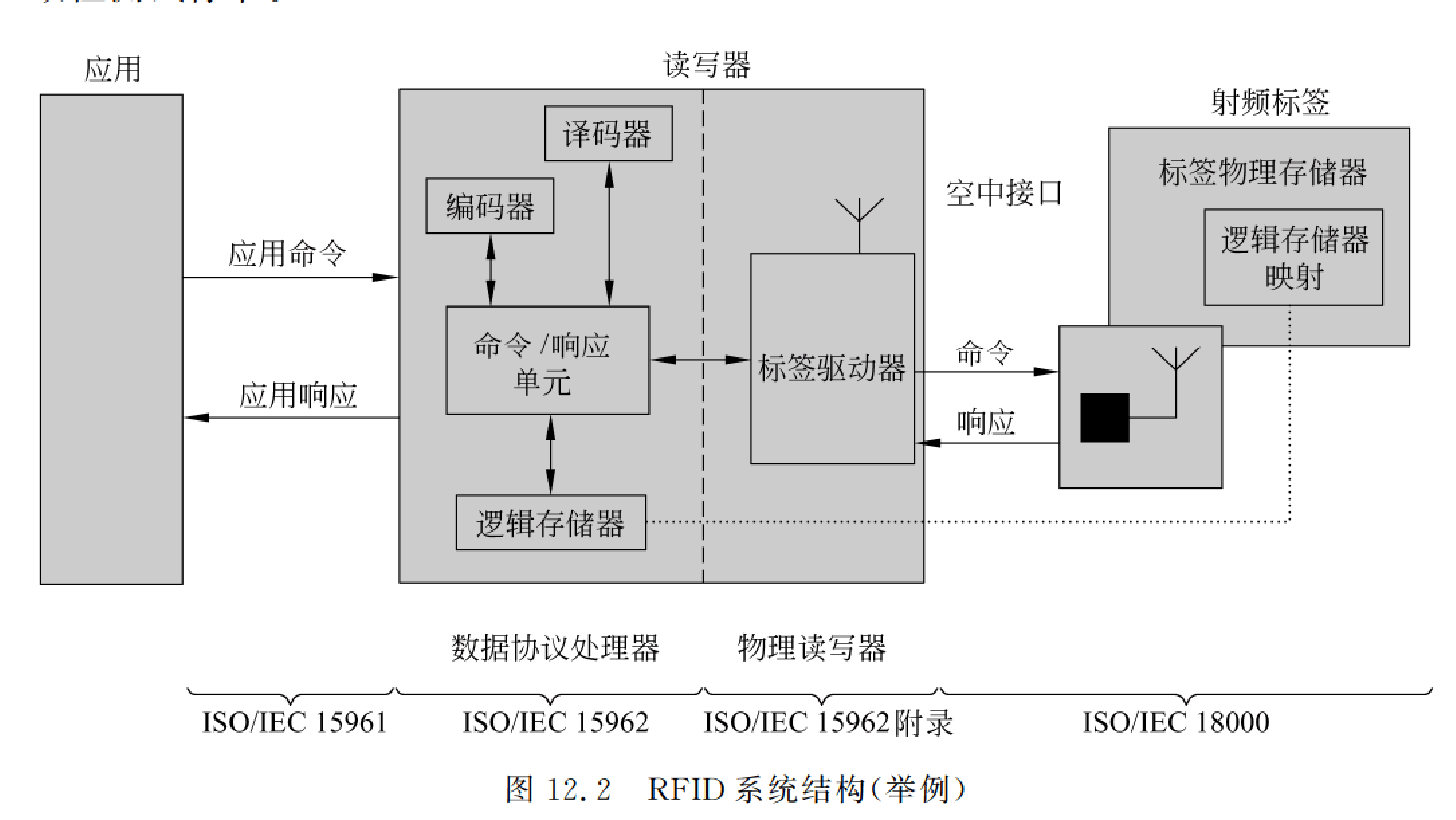


图12.2　RFID系统结构（举例）

12.4　传感器和传感网

12.4.1　传感器

传感器在工业自动化、军事国防和以宇宙开发、海洋开发为代表的尖端科学和工程领域内得到广泛应用，同时与人们生活密切相关的生物工程、医疗卫生、汽车电子、工业、农业、环境保护、安全设置、家用电器等领域同样得到广泛应用。传感器将上述各领域中测量到的各种信号转换成电信号，根据需求进行放大、反馈、微分、存储或远距离操作。可根据各应用领域的实施目标组成相应的传感网。

1. 传感器的作用和组成

传感器是能感受被测件信号并按照一定的规律转换可用信号的器件或装置，通常由敏感元件和转换元件组成。其输出是电信号或其他形式的信息，以满足信息的传输、处理、存储、显示和控制等需要。根据应用需求和环境的不同，有些传感器很简单，仅由一个敏感元件组成，有些传感器的转换元件不止一个，要经过多次转换或用微处理器进行

控制。

在现代工业生产尤其是自动化生产过程中，要用各种传感器来监视和控制生产过程中的各个参数，使机器工作在正常状态或最佳状态，产品达到最好的质量。

现代科学技术的发展进入了新领域，宏观上观察宇宙，微观上要观察微小的颗粒。此外，为了对物质的深化认识，以及开拓新能源、新材料的研究，在相应的超高湿、超低温、超高真空、超强或超弱磁场等环境中，都有相应的传感器。

2. 传感器按照用途分类

(1) 压力传感器。实现工业过程自动化的传感器之一，可测量力和压力，以及负荷、加速度、扭矩等物理量，利用现代半导体的压阻效应或物体的弹性进行测量。

(2) 位置传感器。通过磁性开关来检测气动活塞的位置、机器人系统的高精度定位等，并进行处理。

(3) 液面传感器。容器内的液体表面称为液面，对液面高度进行检测，包括浮球式液面传感器和超声波液面传感器等。超声波液面传感器利用超声波经物体表面反射后产生的信号，根据超声波发出的时间和反射信号的时间差计算传感器到被测液面的距离。

(4) 速度传感器和加速度传感器。检测物体活动的速度和加速度。

(5) 射线辐射传感器。用来检测 X 射线、红外线、紫外线、电磁和核辐射强度等。

(6) 振动传感器。检测物体机械活动的参量，如振荡速度和频率等。

(7) 热敏传感器。利用导体或半导体的电阻率随温度变化的特点，根据传感器测量到的电阻率计算温度。

(8) 其他。还有湿敏传感器、气敏传感器、噪声传感器、重力传感器、真空传感器和生物传感器等。

手机中的重力传感器实现了屏幕图形的自动旋转，便于观看。

上述各种传感器都要对测得的数据进行处理，输出的信号可能是模拟信号、数字信号或开关信号等。

国产传感器以中、低档为主，数字化、智能化、微型化产品欠缺，目前 80%依赖进口。因此要形成从技术开发、设计、生产到应用的完整产品体系。

3. 传感器的通用参数

不同类型的传感器对参数的需求是有差异的，下面介绍常用的参数。

(1) 灵敏度。灵敏度是指传感器输出量与输入量的比例，或者输出的变量和输入的变量的比例。

(2) 分辨率。分辨率是指传感器在规定的测量范围内能够检测出被测量的最小变量。

(3) 线性度。线性度是指传感器的输出量和输入量的测试曲线和直线的差异。

(4) 迟滞。迟滞是指在相同条件下，传感器的正向行程和反向行程的不一致程度。

(5) 重复性。重复性是指在同一工作条件和环境下，测试结果的一致性。

(6) 漂移值。漂移值是指在输入和工作条件不变的情况下，输出量发生变化的值即为漂移值。

4. 物联网中的传感器

物联网中的传感器一般具有信号处理能力，并将输出传递给处理中心进行判断处理，称为智能传感器。

智能传感器一般带有微处理器，具有自检测、自修正、自保护等功能，是由传统的传感器、微处理器和网络接口组成的传感器节点。

12.4.2 传感网

1. 传感网的结构

传感网技术综合了传感器技术、嵌入式技术、现代网络和无线通信技术。传感网结构如图 12.3 所示，包括监测区域的传感器节点、汇聚节点和任务管理节点，传感器节点可通过自组织方式构成网络，传感器节点监测的数据可在监测区域内逐点传输，在传输过程中可能被多个节点处理(如图中的 A、B、C 节点)，再连到汇聚节点。然后通过传感网以外的互联网和卫星到达用户的任务管理节点，形成一个数据传输网络。

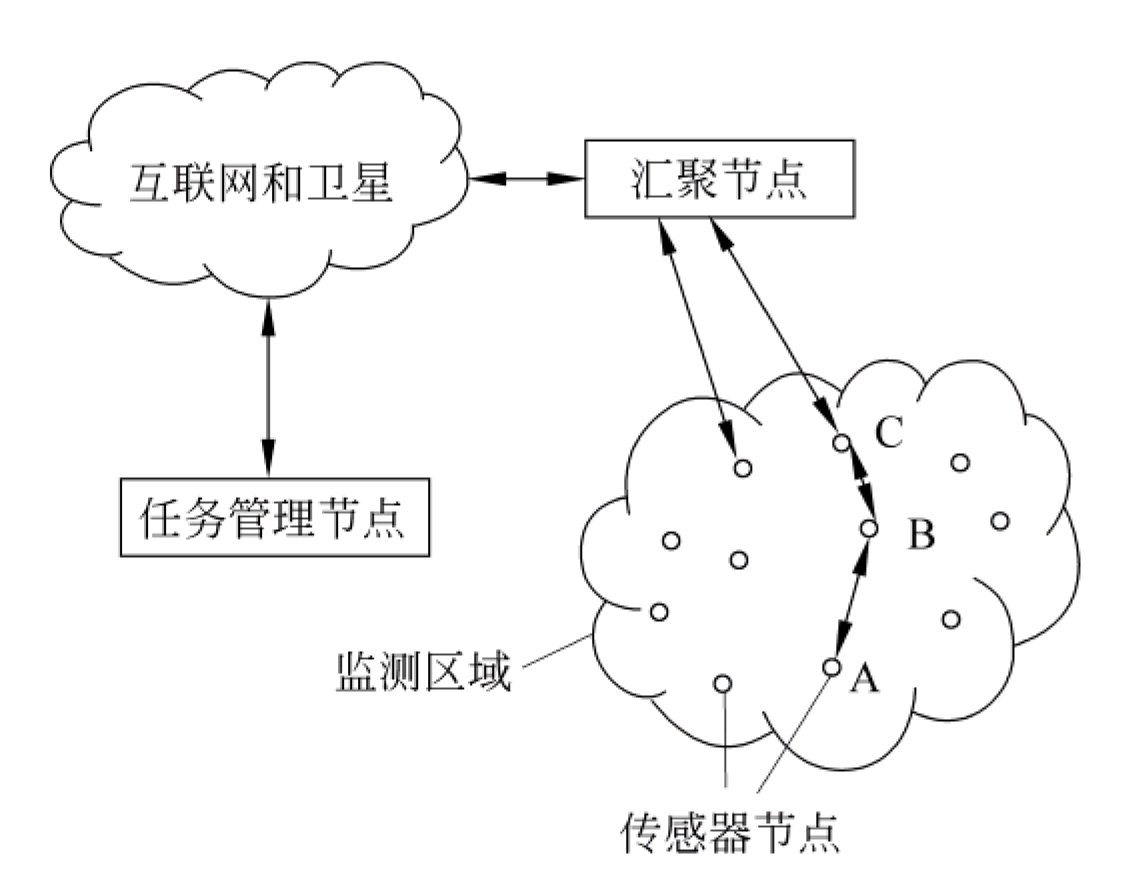


图 12.3 传感网的体系结构(示意图)

按照相互默认的规则，既各尽其职责，又协调地自动形成系统，即为自组织。

2. 物联网中的传感网

传感网(传感器网络)是利用各种传感器(光、电、温度、湿度、压力等)加上中低速的近距离的无线通信技术构成自组织网络，是由多个具有有线或无线通信和计算能力的低功耗的传感器节点构成的网络系统，它一般提供局域和小范围物与物之间的信息交换功能。

3. 传感器节点

目前一个智能手机要用到十几种传感器，一辆高档汽车要用到几百个传感器，而现代化工厂也要用到数以万计的传感器，传感器为人们缔造了智能生活。

汽车是个大型的传感网节点，一个高档汽车有十几个 CPU，有相应的软件程序，电子系统成本占汽车成本的 30%～60%。

汽车传感器由单纯用于发动机上，已扩展到底盘、车身、灯光和电气系统上，常见的有：

进气压力传感器、空气流量计(测量发动机吸入的空气量)、节气门位置传感器(测量

节气门打开角度）、曲轴位置传感器（检测曲轴及发动机转速）、氧传感器（检测排气中的氧浓度）、进气温度传感器、冷却液温度传感器、爆震传感器（检测发动机的爆燃情况）、空调压缩机传感器等。

汽车上用的计算机板称为ECU。

ECU（Electronic Control Unit，电子控制单元），又称“行车计算机”“车载计算机”等，是汽车专用单板机，由微处理机（CPU或MCU）、存储器、输入/输出接口（I/O）、模数转换器（A/D），以及信号整形、驱动等集成电路组成。汽车在运行时，它采集各传感器的信号，进行运算，并将运算结果转变为控制信号给被控制对象。

目前，不但在发动机上应用ECU，其他地方也用到微处理器，如ABS（Antilock Brake System，防抱死制动系统），它在汽车制动（刹车）时，自动控制制动力的大小，使车轮不被抱死，边滚边滑，保证车轮与地面附着力在最大值。还有4轮驱动系统、电控自动变速器、主动悬架系统、安全气囊系统、电控座椅（提高舒适度）、仪表展示、防盗、电动门窗和倒车雷达等处理器。为了在车内传输信号而组成一个网络。

无人驾驶汽车通过“车载传感系统”感知道路环境，自动规划行车路线，并控制汽车到达预定目的地的智能汽车。

车载传感系统用于感知汽车的周围环境、汽车自身的位置及障碍物的位置，控制车辆的转向和行驶速度。

无人驾驶汽车将通过自身的雷达系统检测与前车距离（避免汽车追尾），可自动识别交通指示牌和行车信息，装备雷达、照相机、全球卫星导航等电子设备，集自动控制、体系结构、人工智能、视觉计算等技术于一体。

4. 车联网（Internet of Vehicles）

车联网是物联网技术在交通领域的典型应用。

不同行业、不同联盟对车联网的定义还不一致，例如：

（1）中国互联网校企联盟定义：是由车辆位置、速度和路线等信息组成的网络。通过GPS、RFID、传感器、摄像头、图像处理等装置，车辆对自身环境状态信息采集，运用互联网技术，通过分析处理，计算出各个车辆的运行状态，及时汇报路况和安排信号等。

（2）车联网产业技术创新战略联盟定义：以车内网、车际网和车载移动互联网为基础，按照协定的通信协议和数据交换标准，在车与车、路、行人及互联网等之间，进行无线通信和信息交换的大系统网络，是能够实现智能化交通管理、智能动态信息服务和车辆智能化控制一体化的网络。

12.5 “互联网＋”和《中国制造2025》

12.5.1 互联网＋

互联网是指在全球范围内实现数据的传输。“互联网＋”＝“互联网＋各个传统行业”。利用互联网平台、信息通信技术把互联网和传统行业中的各行各业结合起来，从而创建成新领域。

2015年3月，在十二届全国人大第三次会议上，李克强总理在政府工作报告中提出"制定互联网＋行动计划"推动移动互联网、云计算、大数据等与现代制造业结合，促进电子商务、互联网工业、互联网金融健康发展，引导互联网企业拓展国际市场。7月4日，国务院印发《关于积极推进"互联网＋"行动的指导意见》，推动互联网由消费领域向生产领域扩展，提升产业发展水平，增强各行业创新能力。

2015年12月16日，第二届世界互联网大会在浙江乌镇开幕，在举行"互联网＋"的论坛上，中国互联网发展基金会联合百度、阿里巴巴、腾讯共同发起倡议，成立"中国互联网＋联盟"。2016年12月16日到18日召开第三届世界互联网大会乌镇峰会。大会发布了15项全球互联网领先科技成果：腾讯微信智能生态平台、阿里巴巴商业生态体系的技术应用、百度大脑、华为"麒麟960"手机芯片等国内科技成果，以及特斯拉自动辅助设计系统、IBM人工智能系统、微软的全息眼镜等。在峰会上人工智能、VR（虚拟现实）成为热点。

2011年前后，移动互联网浪潮兴起，从PC互联网向移动互联网过渡，智能手机等智能终端促进各行业的创新。

"互联网＋"使得第三产业的交通、计算机服务和软件业、批发和零售、住宿和餐饮、金融、房地产、租赁、居民服务、教育、医疗、文化和娱乐等行业发生很大的变化。

人工智能（Artificial Intelligence，AI）是计算机科学的一个分支，是研究、开发用于模拟、延伸和扩展人的智能的理论、方法、技术及应用系统的科学。该领域的研究包括机器人、语言识别、图像识别，自然语言识别和专家系统等，应用领域不断扩大。人工智能是对人的意识、思维过程的模拟。从事这项工作的人必须懂得计算机知识、心理学和哲学等，其目标是使机器能胜任一些通常需要人类智能才能完成的复杂工作，而且其目标是不断发展的。

虚拟现实（Virtual Reality，VR）借助计算机系统和相关科学技术，生成在一定范围内与真实环境下的视、听、触觉等方面高度近似的数字化环境，人与数字化环境下的对象相互作用，产生亲临现实环境的感受和体验。随着计算机技术，特别是高性能计算、计算机图形学和人机交互技术的发展，人们在模拟现实世界上达到新境界，包括航空航天、国防军事、装备制造、智慧城市、公共安全、医疗健康、文化教育等方面。VR一体机还存在过重、眩晕、续航、散热等难题。对CPU、GPU和显示屏都提出新的要求。

12.5.2　中国制造2025

1. 2015年5月国务院印发《中国制造2025》的通知

制造业是国民经济的主体，没有强大的制造业，就没有国家和民族的强盛。与世界先进水平相比，我国制造业大而不强，在自主创新能力、资源利用效率、产业结构水平、信息化程度、质量效益等方面差距明显。为了实施制造强国战略，力争通过30年努力，到中华人民共和国成立一百年时，把我国建设成引领世界制造业发展的制造强国。《中国制造2025》是我国实施制造强国战略的第一个十年行动纲领。基本方针是：创新驱动、质量为先、绿色发展、结构优化、人才为本。到2025年，制造业整体素质大幅提升、创新能力显著增强、劳动生产率明显提高，工业化和信息化整合迈上新台阶。到2035年，我国制造业整

体达到世界制造强国阵营中等水平。中华人民共和国成立一百年时，综合实力进入世界制造强国前列，建成全球领先的技术体系和产业体系。

《中国制造 2025》选择十大优势和战略产业作为突破点，它们是新一代信息技术产业、高档数控机床和机器人、航空航天装备、海洋工程装备和高技术船舶、先进轨道交通装备、节能与新能源汽车、电力装备、农业装备、新材料、生物医药及高性能医疗器械。

2. 国家智能制造标准体系建设指南

随着新一代信息通信技术与先进制造技术的深度融合，全球兴起了以智能制造为代表的新一轮产业变革，数字化、网络化、智能化日益成为未来制造业的主要趋势。2015 年年底，工信部和国家标准化管理委员会联合制定并发布了《国家智能制造标准体系建设指南（2015 年版）》（以下简称《建设指南》），从生命周期、系统层级、智能功能建立了参考模型，并提出了涵盖“基础”“安全”“管理”“检测评价”和“可靠性”五类基础共性标准，以及“智能装备”“智能工厂”“智能服务”“工业软件和大数据”“工业互联网”五类关键技术标准。并制定《中国制造 2025》中选择的十大优势和战略产业的应用标准。智能制造标准体系结构如图 12.4 所示，包括“A 基础共性”“B(BA～BE)关键技术”“C 行业应用”。

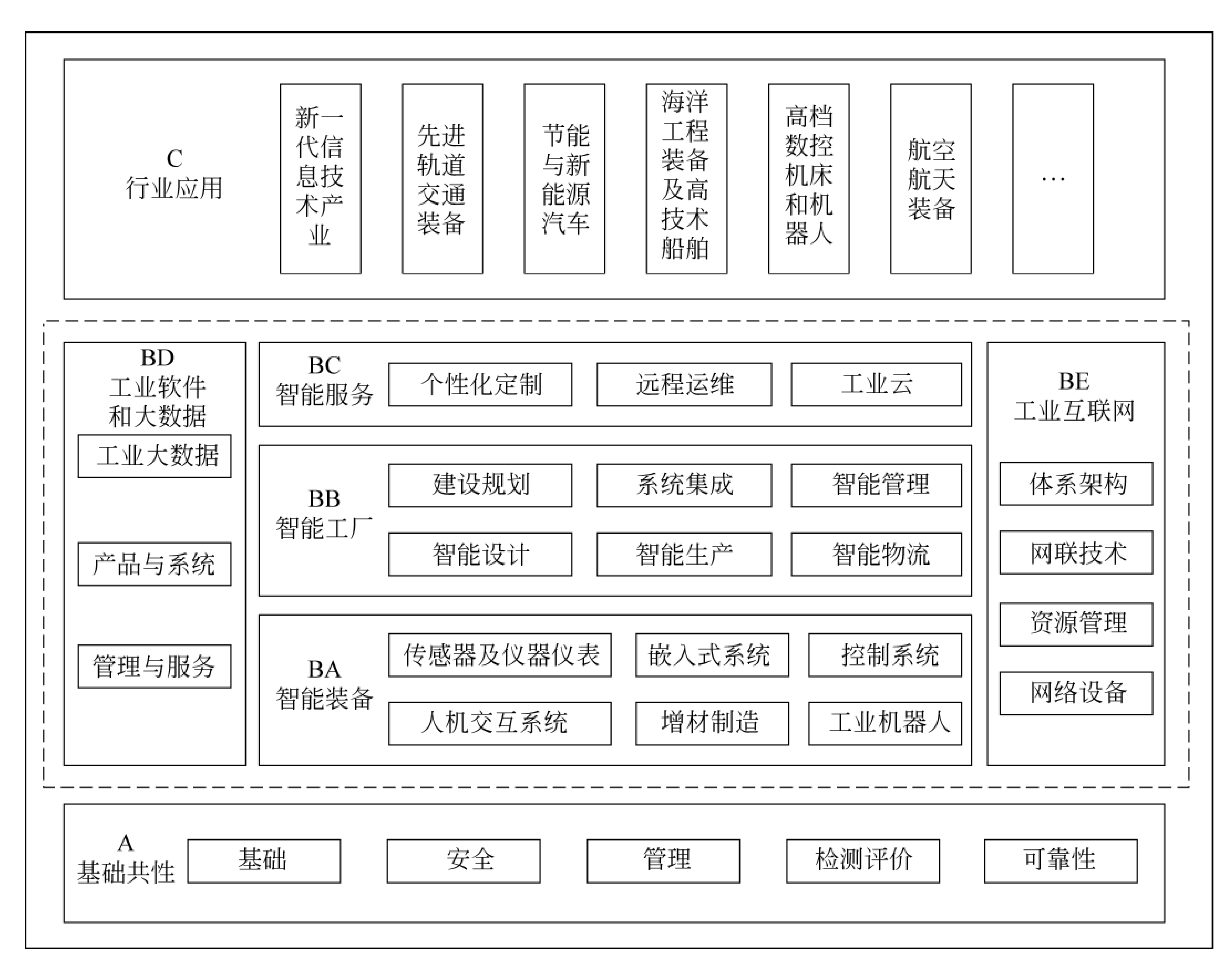


图 12.4　智能制造标准体系结构图

3. 工业革命

18 世纪以来的工业发展：以蒸汽机为动力的时代是第一次工业革命时期；以发电机和内燃机等为代表的是第二次工业革命时期；到 20 世纪四五十年代，以原子能、电子计算机、空间技术和生物工程的发明及应用为标志的是第三次工业革命时期。我们现在正在经历的是“智能制造”新征程。

德国“工业 4.0”是在 2013 年 4 月的汉诺威工业博览会上正式推出的，并逐步上升为德国国家战略，其核心内容为：建设一个网络(信息物理系统)、研究两大主题(智能工厂、智能生产)、实现三大集成(纵向集成、横向集成、端到端集成)。

美国“工业互联网”联盟于 2014 年 4 月成立，是一个开放性的会员组织，促进物理世界与数字世界的融合，实现各厂商设备的数据共享，助力软硬件厂商开发与“工业互联网”兼容的产品，实现仪表、传感器、计算机、网络、云计算系统等物理实体互联。

我国《建设指南》将智能制造定义为将物联网、大数据、云计算等新一代信息技术与设计、生产、管理、服务等制造环节融合。

当传统的产品变成智能产品后，不仅体现在消费者使用时的智能性，也体现在生命周期中。生命周期是指由设计、生产、测试、物流、销售到服务，如 RFID 标签，可以记录产品从设计到服务整个过程的信息，可通过网络跟踪每一件商品的去向。

12.5.3 智能制造关键技术

1. 智能装备

(1) 传感器及仪器仪表是获取自然、应用和生产领域中信息的最主要设备。

(2) 嵌入式系统是嵌入受控设备内部，由专用计算机和执行装置组成，接受计算机发出的命令，执行所规定的操作或任务。

(3) 控制系统是信息化、自动化和智能化的关键。现在流行的现场总线控制系统对生产的控制信息及图像、语音信号等大数据量及传输速度的要求，促使了在工业控制领域内局域网(以太网)和控制网络的结合。

(4) 人机交互系统是用户与系统之间的信息交换。人机交互技术是一个典型的模式识别问题，智能机器通过多种传感器，获取人的表情、手势、语言和(或)血压、心跳等数据，结合当时的环境和上下文信息，识别和理解用户的需求，并予以处理。涉及传感器技术、计算机科学、认知科学、人机工程学、心理学、哲学、多媒体技术和(或)虚拟现实技术等。

(5) 增材制造是通过 CAD(计算机辅助设计)，全程由计算机控制，将材料逐层累加到制造实体零件的技术。由于系统成本高、材料特殊及操作复杂，目前主要应用于科研和工业应用。随着桌面型三维打印(3D 打印)技术的产生，应用范围得到扩展。

(6) 工业机器人取代工业生产中部分劳动者，其发展取决于下列几项技术。

① 传感器融合。移动机器人要有感知功能，单个传感器数据测量存在误差，所以多传感器信息融合是一项关键技术。

② 人机交互。对人的各种动作做出反应，像在人与人之间的交流一样无障碍。

③ 系统集成。集成软件能够实现自主的行为，出现故障时能自我恢复；能有模拟工

业机器人的使用环境，提供关键构件；能建立与实际机器人性能一致的仿真机器人。

④ 定位系统。定位系统是室内外移动机器人不可缺少的组成部分，导航定位技术对提高机器自动化水平具有重要价值。

2. 智能工厂

从设备控制到企业资源管理所有环节的信息快速交换、存储、处理的智能化集成，推动制造企业向新的商业模式和应用模式全方位转型升级。一个新产业的出现，在国家还没有统一标准时，先涉足者将获得更好的收益。

当前，发达国家将智能制造建设作为国家战略，有德国的“工业 4.0”、美国的“工业互联网”、日本的第四期“科技发展基本计划”、韩国的“数字经济”国家战略等。

3. 智能服务

发展面向制造业的智能服务，是推动制造业转型升级、发展智能制造的重要基础。

4. 工业软件和大数据

工业软件是指为提高工业企业的研发、制造、生产管理水平和工业装备性能的软件，也包含处理大数据的软件。条形码、二维码、RFID、工业传感器、工业自动控制系统、智能服务、工业互联网、工业物联网等产生了大量数据，通过处理，加速产品创新、个性化服务、故障诊断与预测、生产线改进和管理等。

12.6 数据中心、大数据与云计算

1. 数据中心

数据中心(Data Center)是指能为客户实现信息查询、处理、存储、传输、交换和管理功能的场所，能对数据进行分析、挖掘、生成、整合和维护。这也是目前提出的大数据(Big Data)技术的实现基础。其基础设施包括服务器、网络、存储设备、软件和开发运行维护的服务人员。

对于高级别的数据中心，其基础设施与服务质量关注如下。

(1) 电力。电力公司冗余的电力资源和线路。数据中心内部安装备用发电机、UPS(不间断电源)等相关冗余设备，以保证电力系统和冷却设备的不中断运行。

(2) 计算机系统。服务器、存储器、网络设备和电信设备等均完全冗余，并保证在出现系统故障时对相关硬件进行实时切换，可以在不中断应用程序的同时，实现对相关程序的性能维护。

(3) 数据。支持海量存储(数据库)及数据的本地和异地备份。提供及时的数据恢复和纠错功能，以保护数据的完整性和正确性。关注数据的使用效率及处理和传输的延迟时间。

(4) 可用性。能够提供每年 365 天、每周 7 天、每天 24 小时不间断应用服务。完全冗余和可容错的电力、计算机、网络和电信设备，冗余的网络带宽服务，可以增强数据中心的可用性。同样适用于为实现业务连续性和灾难恢复准备的备用场所，可以进一步保证服务的不中断运行。

(5) 安全性。数据中心现场拥有 24 小时(日夜不断地)现场电子监视和安全监控系

统。同时，具备保护措施保证计算机系统中用户数据不被泄露、不被篡改。

(6) 灾难及恢复。数据中心配置有效的监测和灭火装置，建筑物理构造坚固，在一定程度上能够抵抗龙卷风、台风、洪水等自然灾害的威胁。建立自然灾害预防和服务功能恢复的备用场所。

(7) 高质量的服务人员和服务水平。数据中心的发展趋势是高度灵活性和适应性，采用虚拟化技术，与大数据、云计算融合。

世界数据中心(World Data Center，WDC)是国际科学研究会下设的全球科学数据组织，有美国 WDC-A、苏联 WDC-B、欧洲与日本 WDC-C、中国 WDC-D 4 个数据中心群。中国于 1998 年加入 WDC。中国有 9 个分中心(括号内为挂靠单位)：海洋学科数据中心(国家海洋信息中心)、地质学科数据中心(中国地震局分析预报中心)、地质学科数据中心(中国地质科学院信息中心)、空间学科数据中心(中科院空间中心)、天文学科数据中心(中科院国家天文台)、气象学科数据中心(国家气象中心)、冰川学科数据中心(中科院寒旱所)、资源环境学科数据中心(中科院地理所)、地球物理学科数据中心(中科院地质地球所)。

2. 大数据

大数据(big data)是指无法在可承受时间范围内，用人脑和常规软件工具进行捕捉、管理和处理的数据集合。

1) 大数据技术

根据应用需求对已掌握的各类大型数据进行专业化处理，包括数据采集、存储、管理、分析挖掘和可视化等技术，整理出帮助企业决策的资讯或对应用有价值的信息。对不同领域、不同企业的不同业务，由于其业务需求、数据分析、数据挖掘目的有差异，所运用的大数据技术和信息系统也可能有相当大的不同。对象、技术、应用三位一体共同发展。对海量和非结构化数据的处理工作量大，无法用单台计算机完成，一般依托云计算的分布式处理、云存储、分布式数据库和虚拟化技术。

2) 数据挖掘

数据挖掘(data mining)又译为资料探勘、数据采矿。一般指从大量数据中，通过算法、搜索出隐藏其中的信息，可通过统计、在线分析处理、情报检索、机器学习、专家系统或模式识别等实现上述目标。专家系统是依靠已经实施的经验和法则生成的系统。模式识别是指通过计算机技术和数学方法来研究模式的自动处理和判读。一般将环境与客体统称为模式。对人类，重点是对光学信息(通过视觉器官)和声学信息(通过听觉器官)识别。市场上的产品有光学字符识别和语音识别系统。

3. 云计算

1) 云计算定义

云计算(cloud computing)还没有统一的定义。现阶段广为用户接受的是美国国家标准与技术研究院(NIST)的定义，其内容为：云计算是按使用量付费的模式，提供可用的、便捷的、按需的网络访问，进入可配置的计算资源共享池(资源包括网络、服务器、存储、应用软件服务)，这些资源能够被快速提供，用户只需投入很少的管理工作，计算由服务供应商进行。

2) 简史

大规模分布式计算技术即为“云计算”概念的起源。分布式计算技术一般是根据用户

的服务需求通过网络将复杂的计算处理程序自动分解成众多较小的子程序，再交给多台服务器所组成的系统，经处理和计算之后将结果回传给用户。

云计算的名词是借用量子物理中的“电子云”概念。云计算是继20世纪80年代从大型计算机到客户机/服务器的大转变之后的又一次巨变，用户不需要了解“云”中基础设施、程序和相应的专业知识等，服务商通过互联网提供可伸缩的、易扩展且具有虚拟化特征的资源。

2006年3月，亚马逊(Amazon)推出弹性计算云服务，2006年8月谷歌(Google)提出云计算概念，2007年10月，Google和IBM在美国大学中推广云计算的科研计划，2010年7月美国国家航空航天局和Rackspace、AMD、Intel和戴尔等厂商共同宣布“open stack”云计算开放源代码计划，后来微软表示支持并采用，思科正式加入“open stack”。

3）云计算的三层次服务

云计算的三层次服务包括基础设施即服务(IaaS)、平台即服务(PaaS)、软件即服务(SaaS)，如图12.5所示。

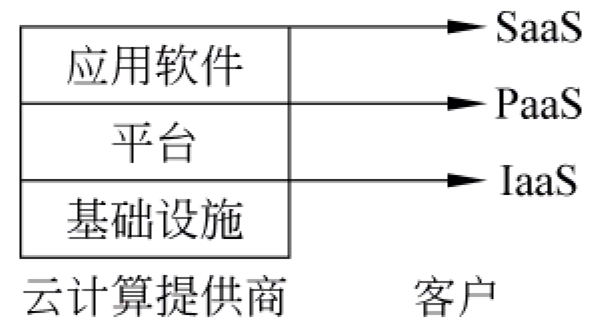


图12.5　云计算服务

(1) 基础设施即服务(Infrastructure as a Service，IaaS)。服务商通过互联网向用户提供基础架构(软件和硬件)，IaaS可以提供计算机服务器、操作系统、存储器、数据库等资源。

(2) 平台即服务(Platform as a Service，PaaS)。平台建立在基础设施上，是服务商将应用软件研发平台租给用户的一种服务，用户可在平台上开发自己的应用软件。

(3) 软件即服务(Software as a Service，SaaS)。服务商通过互联网向用户提供应用软件，用户可以根据实际需求向服务商租用所需的应用软件，用户无须购买、管理和维修软硬件，一切由服务商负责。对于许多中小企业来说，SaaS是采用先进技术的最佳途径。

从技术角度来看，SaaS可以基于PaaS或直接置于IaaS之上，PaaS可以构建在IaaS之上，或者直接构建在物理资源之上，这说明不同服务商之间，其基础设施与平台层之间的分界线并不完全相同，同时3个层次提供的服务内容也有所区别，而且每个云计算服务商不一定能提供3个层次的服务。

4）公有云和私有云

(1) 公有云。由云计算服务商提供的服务即属于公有云，有以下特点。

① 用户享有最优的性价比服务，租用比自购省心廉价。

② 用户需求会随着技术或业务的发展而变，所以阶段性的改变租用的服务功能，对用户来说是一种好办法，可减轻培养人才的负担和快速实现新功能的目标。

③ 服务商可提供全天候服务和数据备份，以及及时处理故障。

(2) 私有云。私有云是企业创建云计算所需的基础设施与软硬件资源，以供本企业或企业内各部门共享并提供服务，其主要优点如下。

① 数据和安全性的有效控制，大型企业(尤其是军方)不会将其关键业务或数据放在公有云上。

② 提供更高的内部服务质量，提供更加稳定可靠和快捷的服务。

③ 可以充分利用企业(尤其是大企业)已有的硬件和软件资源来构建私有云。

5）云计算特点

(1) 超大规模。Google、Amazon、IBM、微软等公司的“云计算”(公有云)已拥有几十万台到一百多万台服务器,企业私有云一般有数百上千台服务器。

(2) 虚拟化。用户使用的资源来自云,不仅是固定的实体,用户还可使用笔记本或手机通过网络服务实现甚至是超级计算的任务。

(3) 高可靠性、通用性、可扩展性。云计算按需服务,为人类进步作贡献,而不是简单的技术提升。

(4) 潜在的危险性。云计算服务还包括数据存储服务,当前掌握在私人企业(服务商)手中,仅提供商业信用。政府机构、商业机构(如银行)要保持警惕,在公有云中处理的数据可能无保密可言。

习题

1. 什么是物联网?
2. 物联网的产生与条形码、传感器和 RFID 标签的应用有关吗?
3. 传感器起什么作用? 经常用到的传感器有哪些? 怎样构成传感网?
4. 一般将物联网体系分为几个层次? 各层的功能是什么?
5. 家中使用的 WiFi 起什么作用?
6. 请解释“互联网+”的含义。
7. 智能制造涉及的智能设备可能有哪些?
8.《中国制造 2025》的目标是什么?
9. 数据中心和大数据的含义和实施方法有什么不同?
10. “云计算”分成哪 3 个层次? 什么是公有云和私有云? 各有什么利弊? 你认为“云计算”的服务前景如何?

第 13 章　互联网、移动通信网、广播电视网

13.1　三网融合的概念

在三网中，首先发展的是互联网，兼有“有线”和“无线”传送数据的能力。随着智能手机的出现，手机除了维持通话的功能外，还继承了平板电脑的功能，这就是后面讨论的移动通信网。近年来，在广播电视领域向用户开放了宽带服务的功能，当前有线电视的信号传输线基本上已连接到楼房内，通过调制解调器后接到路由器，生成 WiFi 信号，最终达到传送数字、语音和影视的目标。本章主要以目前广泛使用的无线 WiFi 技术为基础，将计算机、手机和电视的服务功能融合在一起。但在三网之间仍有功能、性价比的差异，因此融合与竞争并存。

13.2　电磁波频段

在我们的日常生活中，电磁波无处不在。欧美等国家和地区都对电磁波频率的使用实行了许可证制度，中国由国家无线电管理委员会管理。国际上通行的电磁波频段的划分方法如表 13.1 所示。

表 13.1　电磁波频段(波长)的划分

波段名	光波	微　波			超短波	短波 SW	中波 MW	长波 LW	甚长波	特长波	超长波	极长波
波长(λ)	100～1000nm	1～10mm	1～10cm	10～100cm	1m～10m	10～100m	100～1000m	1～10km	10～100km	100～1000km	1000～10 000km	10 000km以上
频率(f)	3000～300GHz	300～30GHz	30～3GHz	3000～300MHz	300～30MHz	30～3MHz	3000～300kHz	300～30kHz	30～3kHz	3000～300Hz	300～30Hz	30Hz以下
频段		EHF 极高频	SHF 超高频	UHF 特高频	VHF 甚高频	HF 高频	MF 中频	LF 低频	VLF 甚低频	ULF 特低频	SLF 超低频	ELF 极低频

波长(λ)与频率(f)的换算公式：

$$\lambda=\frac{c}{f}=\frac{3\times10^{8}}{f}$$

c 为真空中的光速，如当智能卡的工作频率 f 为 13.56MHz 时，$\lambda=\frac{3\times10^{8}}{13.56}=\frac{300}{13.56}=$ 22.1(m)。

光波的频率高于微波，从高到低排列的次序为紫外线、可见光(紫光、蓝光、青光、绿光、黄光、橙光、红光)、红外线。其中红外线在无线局域网和传感器等领域应用较多，其波

长为 780～1000nm。1993 年由 20 多个大厂商成立了红外线数据标准协会(Infrared Data Association,IrDA),是统一了红外通信标准的国际性组织。标准 IrDA1.0 规定的传输率为 115.2Kb/s,IrDA1.1 的传输率是 4Mb/s,并在提高。IrDA 提出的工作距离不超过 3m,工作角度(视角)为 30°,要对准方向,中间不能有障碍物,随着红外通信技术的发展,工作距离在增加。后来兴起的蓝牙技术,有通信距离远、无角度限制等优点,但速度较低、成本高,而且误码率和保密性不如红外通信,因此尚不能全面取代红外通信。平板电脑、手机等设备支持 IrDA。

在本书中涉及的频段应用情况如下。

国际电信联盟(International Telecommunication Union,ITU)为工业、科学、医学(Industrial Scientific Medical,ISM)频域分配了无须授权即可使用的频率范围(见 8.5.2 节)。无线局域网 WiFi 使用的频段中心为 2.45GHz 和 5.8GHz。在第 9 章介绍的非接触式 IC 卡和第 10 章中介绍的 RFID 标签都在 ISM 的范围内。

无线局域网主要使用微波和红外线。允许使用的微波频率为 902～928MHz,2.4～2.4835GHz,5.725～5.825GHz,18.82～19.205GHz。选择的频率要保证不与其他应用已占用的频率相同,以防干扰。

微波信号可以穿越墙壁,这就保证了基于微波的局域网不被限制在一座建筑中,而红外线不会穿越墙壁。

移动通信网与电视网分配到的频率在 13.4 节和 13.5 节中介绍。

13.3 互联网的应用

13.3.1 局域网

计算机技术和通信技术的发展和随后的结合,为最终用户提供了广泛的服务。集成电路技术的飞速发展,促成了计算机硬件价格的下降,性能的提高。高档计算机和普及应用的微机、平板电脑及各种智能终端不断涌现。本节首先讨论用双绞线、电缆或光纤连接计算机的局域网。

1. 拓扑结构

网络中各个站点(计算机或智能终端)相互连接的方法或形式称为网络拓扑,有多种拓扑结构,如星形拓扑、总线型拓扑、环形拓扑等。下面介绍常用的总线拓扑结构。

总线拓扑结构用单根传输线作为传输介质,所有的站点都通过相应的硬件接口直接连接到传输介质上(或称为总线)。任何一个站的发送信号都可以沿着介质传播,而且被所有其他站点有条件地接收。由于介质共享,一次只能由一个站点发送,因此需要采用某种“访问控制策略”来决定下一次哪一个站点可以发送。

图 13.1 所示为总线型拓扑网络,在传输介质上可以采用两种发送技术,即基带传输和宽带传输。

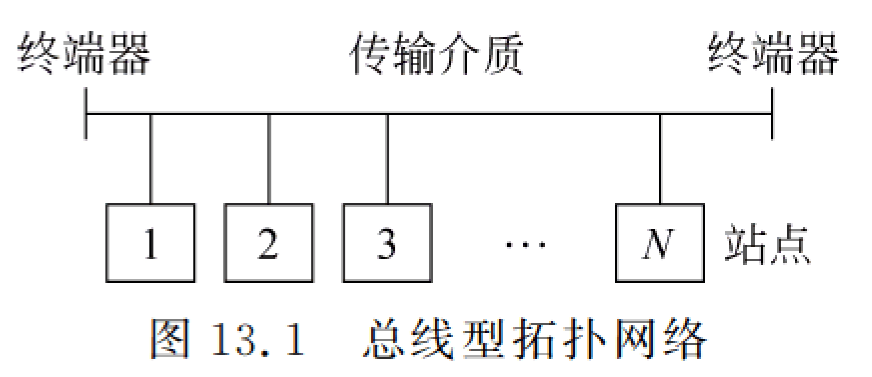


图 13.1　总线型拓扑网络

(1) 基带传输采用数字信号发送,通常用 50Ω 同轴电缆作为传输介质,总线两端加上终端器,以防

止信号反射。其典型实例是以太网(Ethernet)。1980 年 Xerox、DEC 和 Intel 三家公司提出了以太网规范,是世界上第一个局域网产品的规范。传输介质也可采用双绞线。

(2) 宽带传输通常采用 75Ω 电视同轴电缆作为传输介质,用模拟信号发送,一般使用频分调制技术,分成多个频道,分别支持数据通信、电视和无线电信号的传送。

在这里提到的“宽带传输”与 8.2 节中运营商讲的“宽带”根据场合的不同而有所区别。

2. 访问控制策略

当传输介质上有两个或多个站点同时发送信号时,即产生冲突,此时介质上的数据会出错,所以每个站点必须有能力判断冲突是否发生,如果发生,则应等待一个随机时间间隔后重发,以避免或减少再次发生冲突的概率。下面介绍一种用于局域网(以太网)的介质访问方法,即“载波监听多路访问/冲突检测”。

(1) 载波监听多路访问(Carrier Sense Multiple Access, CSMA)。CSMA 控制方案:站点要发送时,首先监听总线,是否已有其他站点在发送信号,如果没有,则可以发送;如果有,则等待一定时间再发送。

一般将数据分成若干个分组,称为数据报或帧。每次发送一个帧。

(2) 冲突检测(Collision Detection,CD)。当两个站点监听总线上没有发送的信号时,如果两个站点同时发送信息,则产生了冲突。一种 CSMA 改进方案(CSMA/CD)广泛应用在局域网中,每个站点在发送帧期间,同时有检测冲突的能力,一旦检测到冲突,立即停止发送,并向总线上发送一串阻塞信号,通知总线上各站点冲突已发生。

3. 以太网

以太网是局域网的主流技术,有传统以太网、快速以太网、千兆位以太网,其传送速率分别为 10Mb/s、100Mb/s 和 1Gb/s。

传统以太网通过 CSMA/CD 方法访问网络,在互联网 TCP/IP 的数据链路层完成防冲突功能。然后将数据帧(在 2.2.2 节中称为数据报)通过物理层传送到传输介质。

数据帧格式包含 7 个域:前置、SFD、DA、SA、数据域(PDU)长度/类型、数据和 CRC,帧格式如图 13.2 所示。



前置	起始帧分界	目的地址	源地址	长度/类型	数据	CRC	
7	1	6	6	2	N	4	字节

图 13.2 帧格式

前置:7 个字节,0 和 1 交替,提醒接收方将有数据传来,并进行同步。

起始帧分界(SFD):1 个字节,为 10101011,这是同步的最后一个字节。

目的地址(DA):6 个字节,接收节点的物理地址。

源地址(SA):6 个字节,发送节点的物理地址

长度/类型(PDU 长度):2 个字节,如果该域＜1518,则为数据长度,如果＞1518,则为数据类型。

数据:46～1500B,如果分组长度＜46B,就需在数据后面加上填充字。

CRC:4 个字节,差错检测信息。

4. 无线以太网

将上面讲到的传输介质用天线取代,并加上调制解调器和路由器即可。在空中传递信息,如目前广泛应用的 WiFi。

13.3.2 网络操作系统

1. 计算机的网络操作系统

网络上各台计算机能方便而有效地共享网络资源,为网络用户提供服务和有关网络规范的软件。

网络操作系统除了应具有通常操作系统的处理器管理、存储器管理、设备管理和文件管理外,还应具有以下功能:在网上有多个用户在争用网上共享的资源,不同用户有不同的作业,因此网络操作系统应支持多用户和多任务;网络上的资源与服务由网上的服务器提供,对平板电脑和智能手机而言,服务器应提供更强的信息存储处理和服务功能;网络软件应实现网络协议(如 TCP/IP)各层次的功能,并遵循各层间通信的协议。

2. 平板电脑和智能手机的操作系统

目前平板电脑的操作系统主要有三大类:Windows、Android 和 iOS。微软的 Windows 和苹果的 iOS 是独家公司研制的操作系统。Android(中文称为安卓)是基于 Linux 的自由开放源代码操作系统。

2005 年 8 月 11 日,Google(谷歌)公司收购成立仅 22 个月的高科技企业 Android 及其团队,2007 年 11 月,Google 与几十家硬件制造商、软件开发商及电信运营商组建"开放手机联盟",将 Android 系统首先应用于智能手机,后来扩展到平板电脑和其他领域,如电视、数码相机和游戏机等。

目前智能手机操作系统的主流为 Windows phone、Android 和 iOS。Android 于 2011 年超过当时流行的 Symbian(塞班)系统。

智能手机除了有电话机和收发短信功能外,还有与平板电脑相似的很多功能,这是因为集成电路、软件和移动互联网高度普及造成的。

下面对一些名词进行介绍。

(1) 自由软件:是一种不受限制的可自由使用、复制、研究、修改和分发的软件,并开放源代码。

(2) 开源软件:开放源代码的软件。有很多程序员在使用开源软件的同时编写专用软件,通过商业化谋取利益。

(3) 免费软件:不付费即可获得的软件,使用者没有复制、研究、修改和分发的自由。该软件的源代码不一定公开。

(4) Linux 操作系统:是免费使用和自由传播的类 UNIX 操作系统,即类似 UNIX,但应用场合比较低档。Linux 的源代码是公开的。如果更改或发展了 Linux 的应用源代码,并作为商用,那么也要公布新的应用源代码。

13.3.3 APP 应用程序

在操作系统之上提供一个平台，供应用程序(Application，APP)开发与使用。

苹果的 iPhone 等智能手机流行，将 APP 指定为智能手机中的第三方应用程序。提供服务的著名商店有 Apple 的 iTunes 商店、Google 的 Google Play，诺基亚的 OviStore 和微软的应用商城。APP 使生产手机的大厂家同时成为服务提供商。

苹果公司的 APP Store 开创了手机软件业务发展的新篇章，除了推出本公司的应用程序外，还为第三方应用软件开发者提供了软件销售平台，使第三方软件开发者的积极性空前高涨，同时促进了用户的兴趣和手机的发售量。到 2013 年 6 月，应用程序数目已达 90 万，在商店下载的应用量为 500 亿次。建立了用户、开发者、苹果三方共赢的商业模式，其中 72%为付费软件，28%为免费应用软件。用户的支付由苹果与开发者按比例 3∶7 分成。

随着互联网的发展，APP 作为盈利模式，为互联网商业界看重，如淘金开发平台、腾讯的微博开放平台、百度的百度应用平台都是 APP 发展的具体表现。

用户界面是基于图形的中文主屏幕用户界面。例如，显示由苹果公司内置的应用程序，以及用户从 APP Store 下载的第三方开发的应用程序，主画面包括以下图标：信息、日历、相片、相机、Safari 浏览器、地图、天气、语音备忘录、笔记、时钟、计算器、设置、iTunes 商店和 APP Store，以及由平板电脑、手机的制造者和使用者下载的 APP。

“微信”是最常用的应用程序之一，于 2011 年由腾讯公司开发和发布，最初是为了即时通信和社交活动，不久增加了购物和支付的商务活动，提供了广泛的城市服务，为人们的衣食住行、购物支付、朋友聊天(语音和视频)、文化娱乐、投资理财等方面提供服务。腾讯公司的微信应用软件，目前主要有 iOS 版、Android 版和 Windows 版，它们之间功能基本相同，但是用户界面存在一些差异。

2017 年深圳市软件行业协会出版了《微信使用教程》(内部教材)，是以苹果公司的 iPhone 和 iOS 平台上运行的微信系统编写的，其他品牌手机不能套用全部操作流程，但可供参考。

13.4 移动通信网

手机是亿万群众拥有的移动通信终端。

13.4.1 移动通信的制式和使用频段

1. 移动通信制式

手机从第 2 代(2G)向第 3 代(3G)、第 4 代(4G)、第 5 代(5G)发展，目前在使用的有 2G、3G、4G 手机，并处于不断淘汰和更新的阶段。从 3G 开始，实现了无线通信和互联网多媒体通信的结合，可处理数据、语音、图像、视频、网页浏览和金融、电子商务等服务，即出现了智能手机。

中国三大移动运营商的移动通信制式如表 13.2 所示。

表 13.2　移动通信制式

移动通信制式	2G	3G	4G
中国移动	GSM	TD-SCDMA	TD-LTE
中国联通	GSM	WCDMA	TD-LTE，FDD-LTE
中国电信	CDMA	CDMA2000	TD-LTE，FDD-LTE

表 13.2 中，TD 为时分，FDD 为频分，TD 和 FDD 表示两种不同的数据传输模式。将数据从手机发送到基站称为上行，手机接收数据称为下行。TD 代表时分双工（或半双工）即上、下行在同一频段上按照时间分配交互传输，而 FDD 是上、下行分配不同频段同时传输。LTE 为长期演进技术（Long Time Evolution），表示 3G 向 4G 演进。

2. 使用频率

1）2G 的使用频率

GSM 900（890～960MHz），上行 890～915MHz，下行 935～960MHz

EGSM（扩展 GSM）1800（1710～1880MHz），上行 1710～1785MHz，下行 1805～1880MHz

2）3G 的使用频率

中国移动　1880～1900MHz，2010～2025MHz

中国联通　1940～1955MHz（上行），2130～2145MHz（下行）

中国电信　1920～1935MHz（上行），2110～2125MHz（下行）

后来对 3G 频段作了扩展：806～960MHz，1710～1885MHz，2500～2690MHz

3）4G 的使用频率

中国移动　TD-LTE 1880～1900MHz，2320～2370MHz，2575～2635MHz

中国联通　TD-LTE 2555～2575MHz，2300～2320MHz

FDD-LTE 1755～1765MHz（上行），1850～1860MHz（下行）

中国电信　TD-LTE 2370～2390MHz，2635～2655MHz

FDD-LTE 1765～1780MHz（上行），1860～1875MHz（下行）

从以上频段可看出，TD-LTE 不分上行和下行，FDD-LTE 有上行和下行，而且在相应的频段中，上行频率低于下行频率。在实践中下行传送的数据量大于上行，表现在下行传送网页、微信、电视等。

频段的划分过程由国际管理部门分配到国家的管理部门，再发放牌照到运营商。

13.4.2　移动通信架构

1. 移动终端（如手机）与基站进行通信

基站是建在外面的铁塔，由天线、发射/接收设备、信号处理器等部分组成，手机通话时都要占用一个频道，假如通话的人多了，会出现通话阻塞的现象，为此在指定的通信区域内可建立多个基站，以改善通话情况，举例如下：

将某通信大区划分成 72 个小区，建立了 72 个基站，又将其中的 12 个小区组成一个小区群，共有 6 个小区群，假如从国家分配给它的使用频段可分成 300 个频道（按频道顺序增加相同的频率）。

1	2	3	4	1	2	3	4
5	6	7	8	5	6	7	8
9	10	11	12	9	10	11	12
1	2	3	4	1	2	3	4
5	6	7	8	5	6	7	8
9	10	11	12	9	10	11	12
1	2	3	4	1	2	3	4
5	6	7	8	5	6	7	8
9	10	11	12	9	10	11	12

图 13.3　多个基站的示意图

图 13.3 所示为多个基站示意图,图中有 6 个小区群,每个小区群用小区 1,2,3,…,12 表示,每个小区的地面几何形状为小方块。每个小区群都用到了 300 个频道,所有小区群的 1 号小区基站工作于相同的频率下,因为各个 1 号小区的基站相隔距离较大,而电磁波起作用的范围有限,因此不会对其他小区群的 1 号小区造成干扰。同样各小区群的 2 号小区也工作于相同的频率……直到 12 号小区。由于每一频道能重复使用 6 次,因此在理想情况下,原供 300 个用户同时通话的大区,可供 1800 个用户同时通话。

在图 13.3 中,小区基站与小区(小方块)边缘的距离并不完全相同。为照顾边缘远距离用户通话,增加了每个小区电磁波起作用的范围,而造成相邻小区之间的电磁波覆盖,这是缺点。实际使用的不是小方块,而是正六边形,酷似蜂窝的结构,如图 13.4 所示,能完整且基本无重叠地覆盖整个地区。

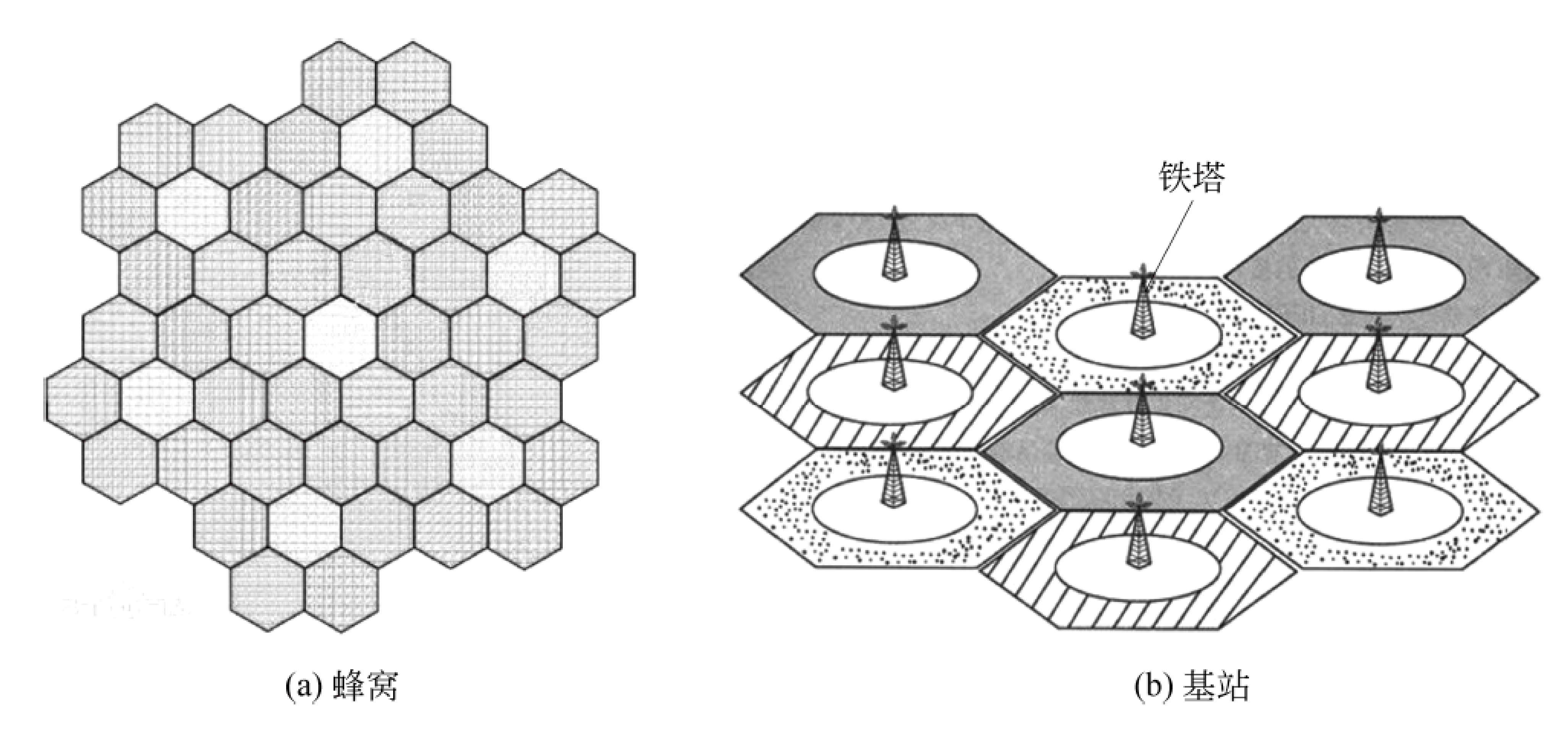


图 13.4　蜂窝和基站

蜂窝网由移动终端、基站和网络子系统组成,无线局域蜂窝网络基于 IEEE 802.11 a/b/g 标准,但频率可扩展。手机可将无线通信与国际互联网等多媒体通信相结合。

加强基站发射功率可以扩大基站到终端(如手机)的覆盖距离。在基站的机房内设置有放大器,以提高发射功率,在塔顶安置低噪声放大器,以提高基础接收的灵敏度。

2. 无线通信(微波通信与卫星通信)

微波通信的地面传送距离可达几十千米,超过几十千米要在地面建立微波中继站。

卫星通信利用人造地球卫星作为中继站,为地面上的两个或多个地球站之间或两个移动体之间建立微波通信联系。卫星通信系统由卫星和地球站两部分组成。

在地球赤道上空约 36 000km 的太空中。围绕地球的圆形轨道上运行的通信卫星称为静止卫星、固定卫星或同步卫星,因为它与地球自转同步,在地面上看如同静止不动一样。只要有 3 颗经度相隔 120°的均匀分布卫星,就可以覆盖全球。

卫星起中继站作用,即把地球站发送来的电磁波经放大后,再返送回另一个或多个地球站,故卫星通信易于实现越洋的洲际通信和广播工作方式,卫星通信频率为 1~10GHz,即微波频段。为适应发展的需要,分配了最高的频段。

卫星通信的优点:通信距离远,不受复杂地球条件的限制,可在大面积范围内实现电视节目、广播节目、新闻的传输和数据的交互,易于实现多地址传播的多种业务功能。

卫星通信的缺点：传输延时大(500～800ms)，高纬度地区难以实现通信，同步轨道上不能无限制地增加卫星数量，太空中的某些现象会影响卫星通信。

3. 全球定位系统

全球定位系统(Global Positioning System，GPS)是指在全球范围内实时进行定位、导航的系统，可以提供车辆定位、防盗、反劫、行驶路线监控和呼叫指挥等功能，要具备GPS终端、传输网络和监控平台。

GPS导航系统以全球24颗人造卫星为基础，它由三部分组成：一是地面控制部分，由主控站、地面天线、监测站和通信辅助设备组成；二是空间部分，由24颗卫星组成，分布在6个轨道平面(其中3颗为备用卫星)；三是用户装置部分，由GPS接收机和天线组成。卫星的分布使得在全球的任何地方和任何时间都能观测到4颗以上卫星，卫星位于距地表20 020km的上空，运行周期为12小时。工作的频率有 $f_1=(1572.42\pm1.023)$MHz、$f_2=(1227.60\pm1.023)$MHz，$f_3=(1176.45\pm1.023)$MHz。

GPS接收机根据用途分为车载式、船载式、机载式、星载式、弹载式。已有多种产品适应相应的GPS应用需求，选购时要注意软硬件配置，举例如下。

(1) GPS在汽车导航和交通管理中的应用。汽车导航系统由GPS导航与电子地图、无线电通信网络、计算机车辆管理信息系统等相结合，实现车辆跟踪和交通管理等功能。

(2) GPS在导航仪中的应用。某产品的核心功能如下。

① 地图查询。在操作终端上搜索目的地位置，记录常去的地方位置或附近的加油站、宾馆、银行等。

② 路线规划。根据终端上设定的起始点和目的地，自动规划一条路线。可设定是否要经过某些途径点或避开某些途径点。

③ 自动导航。语音导航、画面导航或重新规划路线。

全球四大导航系统如下。

(1) 美国GPS系统。24颗卫星分布在6条交叉相隔60°的轨道面上，精度约10m，军民两用。

(2) 俄罗斯“格洛纳斯”系统。24颗卫星组成，精度约为10m，军民两用。

(3) 欧洲“伽利略”系统。30颗卫星组成，定位误差不超过1m，主要为民用。

(4) 中国“北斗”系统。由5颗静止轨道卫星和30颗非静止轨道卫星组成，2012年成功将最后一颗卫星送入预定轨道。

13.4.3 第5代(5G)移动通信

5G是4G之后的延伸，现处于研发阶段，估计在2019年发布国际5G标准，2020年可以提供产品。

2015年6月，国际电信联盟ITU确定了5G的名称、场景和时间表。2016年“国际主流移动通信标准组织”启动标准化工作。5G发展的主要驱动力是移动互联网和物联网。

5G的技术指标：极高的数据传输率(可达1Gb/s至几十Gb/s)，极高的数据流量密度(几十(Tb/s)km^2)，海量的低功耗物联网和垂直行业(如金融网、车联网)应用，低延时

和高可靠性。例如，1s 可下载一部高清电影。

5G 技术创新源自天线和网络，措施如下。

① 大规模天线阵列。增加天线数可支持几十个独立的数据空间流。

② 超密集组网。增加基站密度。

③ 新型多址。发送的信息采用几种多路存取（如空分、时分、频分和码分）方式，叠加传输。

④ 多频段接入。采用多个频段，提高传输速率。

⑤ 提高网络传输速率。5G 比 4G 提高 100 多倍。

注： 数据单位从低向高变化序列为 1、K、M、G、T、P……其中 1K＝1000＝10^3，1M＝1000K，1G＝1000M，1T＝1000G，1P＝1000T，实际上 1000 应以 2^{10}＝1024 取代之。

2016 年 5 月 31 日，第一届全球 5G 大会在中国召开，以“构建 5G 技术生态”为主题，旨在引导全球统一 5G 标准，促进全球 5G 产业及应用发展。由中国 IMT-2020（5G）推进组、欧盟 5GPPP、日本 5GFE、韩国 5G 论坛和美国 5G Americas 共同主办。

2016 年 11 月 9 日到 10 日，第二届全球 5G 大会在意大利罗马召开。中国、欧盟、美国、日本和韩国为主办单位，以“使能 5G 生态圈”为主题，并围绕政策、频谱、技术、标准和产业等 5G 生态建设进行探讨，取得积极成果。

5G 频段：3.5GHz 已在国际上取得共识，高频段将在 2019 年世界无线大会解决。美国联邦通信委员会 FCC 准备将 28GHz、37GHz、29GHz 授权（分配）给本国企业。

13.5 广播电视网

1. 宽带服务

2016 年 5 月 5 日工信部向中国广播电视网络公司颁发了基础电信业务牌照，公司获准开展两项基础电信服务：全国范围内经营互联网国内数据传送功能和国内通信设施服务业务。当前在宽带服务市场具备了与三大基础电信运营商（中国移动、中国联通、中国电信）等同的业务经营权，成为第四大电信运营商。宽带服务是广电网络由 TV 向多业务服务迈出的第一步。

有线电视基本上已可发送到楼内每户家中，解决了“最后一公里”问题，即使是农村和边远地区也在不断推进。

宽带服务的入户方式：用户购置宽带服务（如从北京歌华有线电视网络公司）后，由该公司进户装上调制解调器，然后由用户接上无线路由器（WiFi）即可。目前各省市的有线电视企业都是独立经营的。广电网络全行业内部应该一致行动、联合推广。

2016 年第一季度，广电总局提出：加快推进网络的双向化、宽带化、智能化；加快推进全国有线电视网络的融合、互联互通平台的建设、网络统一管理的运营和网络业务的开发。并明确 700MHz（698～806MHz）频率可用于今后的 LTE 网络部署。

2016 年 11 月，广电国网发布了《中国广电“TV、宽带、无线”全业务融合建设运营规划》。

广电总局和工信部是平级的国家机构，宽带服务的开展将导致双方进一步的合作和竞争。

2. 有线电视(数字电视)各电视台的频道划分

表 13.3 所示为按中心频率增加顺序列出的频道号。

表 13.3　中国有线电视频道划分

频道号	中心频率/MHz	频道号	中心频率/MHz
Z1	115	DS13～DS24	474～562
Z2～Z7	123～163		
DS6	171	Z38～Z42	570～602
DS7～DS11	179～211		
DS12	219	DS25～DS56	610～858
Z8	227	DS57～DS68	866～954
Z9～Z39	235～459		

在表 13.3 中,Z2～Z7 的 6 个频道号被分配的中心频率分别为 123MHz、131MHz、139MHz、147MHz、155MHz 和 163MHz,并可供 DS7～DS11、Z9～Z37 等通道号参考。

频道号用 Z1～Z42、DS6～DS56 表示,每个频道占用的带宽为 8MHz。例如,中央电视台第 1 套频道 DS11 的中心频率为 211MHz(207～215MHz),第 3 套频道 DS18 的中心频率为 514MHz(510～518MHz)。

3. IPTV(Interactive Personality TV)

交互式网络电视。是利用宽带有线电视网的基础设施,以家用电视机为主要终端电器,集互联网、多媒体、通信等技术于一体,向家庭用户提供包括数字电视在内的多种交互式服务。

用户在家中可以有 3 种方式享受 IPTV 服务:计算机;网络机顶盒+电视机;移动终端(手机、iPad 等)。有线数字电视机具有频分制、定时和单向传播的特点,IPTV 则可完成视频点播节目,它采用高效的视频压缩技术提高收视效果,它能根据用户的选择配置多种多媒体服务功能,包括数字电视节目、可视 IP 电话、电子邮件,以及多种在线咨询、娱乐、教育和商务功能,集语音、数据、视频于一体,融互联网、多媒体、通信、广播电视于一体。IP 机顶盒实现了视频、语音和数据三者的融合。

发展数字电视是国家早就规划的,IPTV 是在众多的电视节目中增加一个节目频道,并不替代有线数字电视或卫星电视。

IPTV 的服务主要是收费的,因此快速普及还存在问题。

4. 智能电视

类似于智能手机,应实现全开放式平台,基于操作系统和互联网,可自行安装和卸载各类应用软件。但具有大屏和手机输入方式差异的特点,4K 超高清出现,其分辨率为 3840 像素×2160 像素,是全高清(1920 像素×1080 像素)的 4 倍。

智能电视集双向人机交互功能,可实现网络搜索、IP 电视、视频点播、数字音乐、网络新闻、网络视频电话、录制电视节目、播放卫星和有线电视节目,顺应了电视机“高清化、网络化、智能化”的趋势。

操作系统以 Android 为主,其次为 Windows。Android 是为移动终端推出的,完善地

移植到电视机中有一定的工作量。

智能电视尚处于发展的初期,从智能电视机的应用程序商店中能选择的应用程序数量还很少。

集成电路组成了电子控制终端和计算机,并实现了互联网的功能,为军用和民间各行业的应用发挥重要的作用。移动通信网和广电网也都向智能化性能发展和实现,除了保持和提高原有的功能外,还具有一般计算机的功能,并扩充了计算机的应用范围。例如,当物联网参与线上线下(Online to Offline,O2O)营销时,其工作流程如下:用户进入智能手机的购物 APP,在网上认购商品,扣除用户金融卡(或第三方)上的金额,然后进行“物流”处理,最后将商品送到用户手中。线上是指在网上进行的活动,线下是在现实环境下进行的活动。

固定或移动设备、有线或空中射频传输信息,将根据应用需求、技术水平和成本等因素进行选择和研发。

今日在军事、经济、科技、应用、产品快速发展的情况下,要适应这种变化。

习题

1. 电磁波频段的分配,受国际和国家无线电管理机构控制,为什么?
2. 家中使用的 WiFi 与互联网的关系是什么?当前在我国经营服务的有哪些大经营商?
3. 叙述 2G 手机、智能手机和平板电脑在功能、技术和发展进程之间的相互影响,以及智能电视实现的期望。
4. 在通信数据传送中,“上行”和“下行”是什么意思?目前在广播电视领域中,主要是单向传输还是双向传输?发展前景如何?
5. 你对三网融合的前景有什么看法。

第 14 章　物联网和智能卡的应用

在我国,智能卡的应用范围广,发行量大,目前在我国非接触式 IC 卡一般遵循 ISO/IEC 14443 标准。RFID 标签和传感器在物联网中广泛应用。

14.1　中华人民共和国居民身份证

第二代居民身份证上印有持卡人的姓名、照片和生日、地址等登记项目。

1. 身份证号码

第二代居民身份证号码共 18 位。

(1) 第 1、2 位数字表示所在省(直辖市、自治区)的代码。

(2) 第 3、4 位数字表示所在地级市(自治州)的代码。

(3) 第 5、6 位数字表示所在区(县、自治县、县级市)的代码。

(4) 第 7～14 位数字表示出生年、月、日。

(5) 第 15、16 位数字表示所在地的派出所代码。

(6) 第 17 位数字表示性别,奇数表示男性,偶数表示女性。

(7) 第 18 位数字是校验码,用来检验身份证的正确性。校验码由统一公式计算出来,计算的结果在零与拾的范围内,用数字 0～9 和 X 来表示,X 是罗马数字,代替数字 10,由此保证校验码为 1 位,身份证号码总共为 18 位。校验码的计算方法(步骤)如下。

① 身份证号码的第 1～17 位分别乘以不同的系数。

第	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	位
系数	7	9	10	5	8	4	2	1	6	3	7	9	10	5	8	4	2	

② 将各位相乘的结果再进行相加操作。

③ 将相加的结果除以 11,得余数;余数为 0～10 的一个数字。

④ 将余数进行简单变换,即为身份证号码的第 18 位,变换关系如下:

余数:	0	1	2	3	4	5	6	7	8	9	X	
移位:	2	3	4	5	6	7	8	9	X	0	1	循环左移两位
变换后:	1	0	X	9	8	7	6	5	4	3	2	高低位互换

举例:假设身份证号为 3 4 05 24 19800101 00 1X,对前面 17 位进行处理(步骤 1、2)。

$$\begin{aligned}\text{相乘、相加的结果} &= 3\times7+4\times9+0+5\times5+2\times8+4\times4+1\times2+9\times1+8\times6+\\&\quad 0+0+1\times9+0+1\times5+0+0+1\times2\\&=189\end{aligned}$$

除以 11 得余数:189/11＝17＋2/11,即余数为 2(步骤 3)。

余数经变换后为 X,即第 18 位为 X(步骤 4)。

当持卡人使用身份证时,读卡机对身份证号码进行核算,如果校验码正确,则认为身

份证是合格的;否则认为卡内存储的身份证号码有误或是伪造的。卡内没有设置密码,对持卡人的身份仅能对照片进行人工观察。

2. 技术特点

(1) 使用非接触式IC卡,天线和芯片都封装在卡内,存储器容量较大,写入的信息可划分安全等级,分区存储(姓名、地址、照片等),如地址变动可予以修改,而身份证号码则不能修改。过去身份证有重号现象,但二代身份证已予以解决,现在全国所有人的号码都不相同。证件读写单位按照管理规则进行授权。证件信息的采集和传输采用数码照相和计算机技术,证件制作和管理实行严密的内部管制。用证部门可使用计算机网络核查,有效使用人口资源,实现信息共享。

(2) 防伪能力。采用卡内机读信息的防伪和证件表面的印刷防伪。芯片使用特定的密码算法,起到防止伪造证件或篡改机读信息的作用。

3. 注意措施

(1) 增强用证时验证持卡人身份的能力。

(2) 开发适应各个社会相关部门机读身份证内容的读卡器。

(3) 身份证被盗或伪造的非法使用。

(4) 人名、地名中的生僻字处理。

第三代身份证:公安部规定,2013年起,在全国由点到面逐步在身份证中登入指纹信息(首次申领、换领或补领身份证的公民),凡是尚在有效期的第二代身份证仍可正常使用。

只登入双手大拇指的指纹。

14.2 中国金融集成电路卡规范(电子钱包/电子存折)

《中国金融集成电路(IC)卡规范》(JR/T 0025)中的金融IC卡是指以IC卡为载体、由商业银行向社会发行的、具有消费信用、转账结算、存取现金等全部或部分功能的信用支付工具。

《中国金融集成电路(IC)卡规范》(JR/T 0025)包括电子钱包/电子存折、借记/贷记卡、非接触式金融卡和小额支付规范。

本节讨论的规范由中国人民银行于2005年提出,是行业标准,其代号为JR/T 0025—2005,业界简称PBOC 2.0,并于2010年进行了修改。

PBOC是中国人民银行(The People's Bank of China)的英文缩写。实现电子钱包/电子存折的原理和方法可参阅本书的第3章到第6章。

2002年,经国务院同意,在中央人民银行的领导下,各商业银行联合起来,成立中国银联,到2015年第一季度,银联卡已在境外150个国家和地区使用。

14.2.1 电子钱包/电子存折卡的触点和传输协议

电子钱包(Electronic Purse,EP)/电子存折(Electronic Deposit,ED)应用为同一类应用,两者在卡片和终端处理流程上基本相同,主要区别为:电子钱包应用支持消费、圈存

等交易，消费无须提交个人密码，卡片中的消费明细为可选；电子存折应用支持消费、取现、圈存、圈提和修改透支限额等功能，消费必须提交个人密码，卡片中的消费明细为必选。密钥管理系统在中国人民银行统一管理下建设，并与 EMV 标准的借记/贷记应用兼容。EMV 为 Europay、Mastercard、VISA 的缩写。

1. 卡的触点和数据的传送

IC 卡触点：不使用 C4 与 C8(可不设置这两个触点)；不需要外加编程电压 VPP。

在卡片操作过程中，数据通过 I/O 触点在读写器和 IC 卡之间以异步半双工方式进行双向传送。

1）位持续时间

在 I/O 上的位持续时间被定义为一个基本时间单元 etu。复位应答期间的位持续时间称为"初始 etu"。初始 etu＝$(372/f)$s＝372 个时钟周期。复位应答后的位持续时间称为当前 etu，当前 etu＝$\frac{F}{D}\frac{1}{f}$s。本规范仅支持 $F=372$ 和 $D=1$，因此初始 etu 等于当前 etu，均为$(372/f)$s。

2）字符帧

参见第 4 章。

读写器与 IC 卡之间的传送顺序(即高位先送还是低位先送)由复位应答回送的 TS 字符确定。

2. 复位应答 ATR

在复位应答过程中，两个连续字符的起始位下降沿之间的最小时间间隔为 12 个初始 etu，最大时间间隔是 9600 个初始 etu。

在复位应答期间，IC 卡应在 19 200 个初始 etu 内发送完所有要回送的字符(从第一个字符 TS 起始位下降沿开始计算)。

在复位应答期间回送字符的个数和编码随传输协议和所支持的传输控制参数值而异。本规范支持两种协议($T=0$ 和 $T=1$)，一张卡只支持其中的一种协议，如果 ATR 中的 TD_1 不存在，则使用$T=0$协议。

对于采用 $T=0$ 异步半双工字符传输协议的 IC 卡，其回送字符如表 14.1 所示。

表 14.1　$T=0$ 时的 ATR

字　符	值	备　　注
TS	'3B'或'3F'	说明正向或反向约定
T0	'6X'	TB_1 和 TC_1 存在，X 表示历史字节个数
TB_1	'00'	不使用 VPP
TC_1	'00'到'FF'	指明所需额外保护时间的数量，'FF'值表示两个连续字符的起始位下降沿之间的最小延时为 12etu

对于采用 $T=1$ 异步半双工传输协议的 IC 卡，其回送字符如表 14.2 所示。

表 14.2　$T=1$ 时的 ATR

字　符	值	备　　注
TS	'3B'或'3F'	指明正向或反向约定
T0	'EX'	TB_1 到 TD_1 存在，X 表示历史字节个数
TB_1	'00'	不使用 VPP
TC_1	'00'到'FF'	指明所需额外保护时间的数量，FF 表示两个连续字符的起始位下降沿之间的最小延时可减少到 11etu
TD_1	'81'	TA_2 到 TC_2 不存在，TD_2 存在。使用 $T=1$ 协议
TD_2	'31'	TA_3 和 TB_3 存在，TC_3 和 TD_3 不存在。使用 $T=1$ 协议
TA_3	'10'到'FE'	表示 IC 卡信息域大小的初始值
TB_3	低位半字节 $b_4 \sim b_1$ 高位半字节 $b_8 \sim b_5$	$b_4 \sim b_1$，指定分组内相邻字符间的最大时间 $b_8 \sim b_5$，卡接收最后一个字符到卡发送字符间的最大时间
TCK	异或值	校验字符

14.2.2　EP/ED 的文件结构、应用选择和应用文件

1. 文件结构

数据文件中的数据结构以记录方式或二进制方式(透明结构)存储。本规范定义了应用文件结构，这些应用称为“支付系统应用”。在 MF 下设置有支付系统目录(EF)和应用专用文件(ADF)。

1) 应用专用文件

应用专用文件(Application Dedicated File，ADF)是指一个 ADF(应用 DF)对应一个应用，是一个 AEF(应用基本文件)或多个 AEF 的入口点。ADF 是一个包含其文件控制信息的文件，可通过它来访问 EF 和 DF。在卡中处于最高层的 DF 称为“主文件 MF”。

2) 基本文件

一个基本文件(Elementary File，EF)包含有一个或多个原始 BER-TLV 数据对象。在选择了某一应用后，EF 只能通过其短文件标识符(SFI)进行查询。

3) 卡片内部结构示例

如图 14.1 所示，图中卡片支持电子存折/电子钱包、磁条卡(Easy Entry)及两个没有定义的其他应用。

2. 应用选择

所有应用都唯一地由一个应用标识符标识。

1) 应用标识符的编码

AID 的结构包括如下两部分内容(在第 4 章历史字符中说明)。

(1) 一个经过注册的应用提供者标识符(Registered application provider IDentifier，RID)，长度为 5B，它唯一地标识应用提供者。

(2) 一个可选域，由应用提供者定义，长度为 0～11B，被称为“专有应用标识符扩展

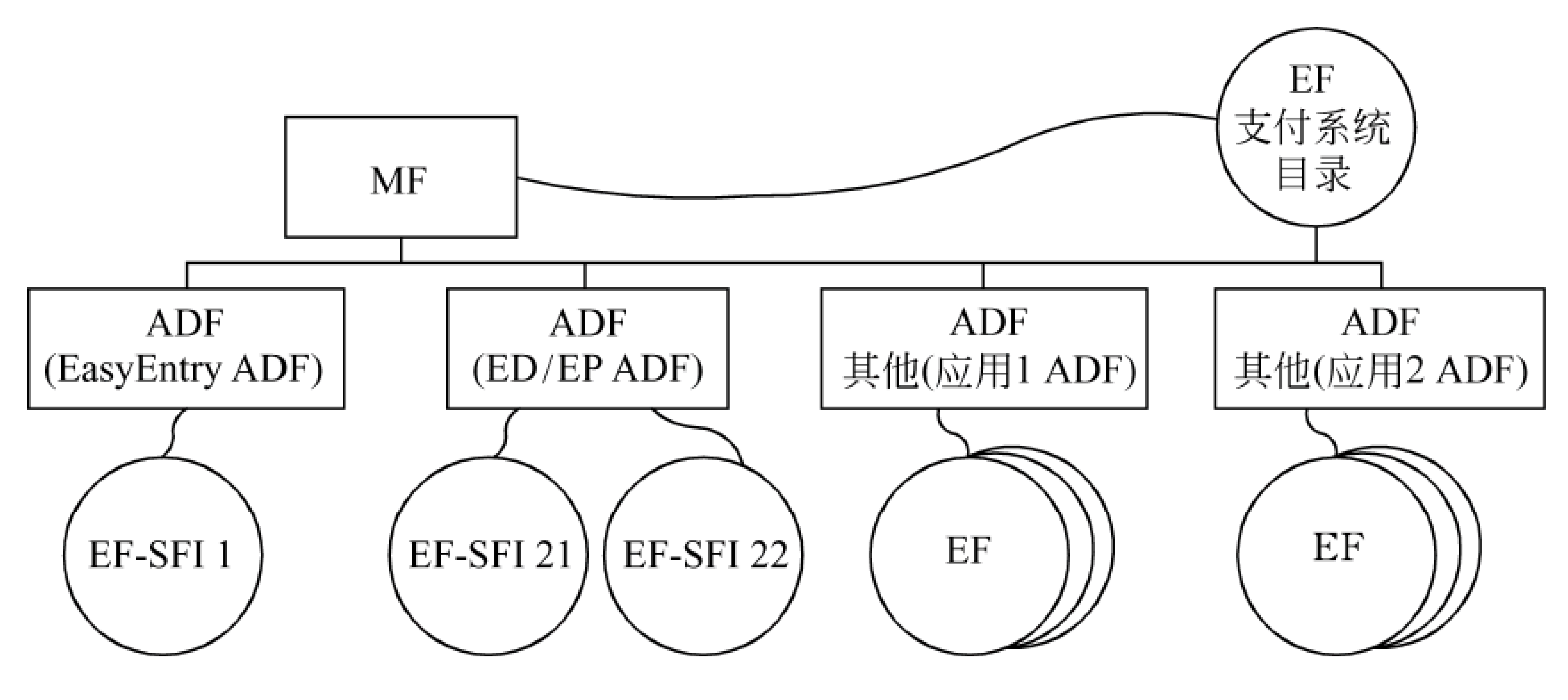


图 14.1　卡片内部结构示例

码”。该域的含义只对特定的 RID，不同 RID 下的 PIX 不需要唯一。

2）支付系统的目录

支付系统目录是一个线性文件，用 1～10 个的短文件标识符标识。目录文件是列出目录里所包含文件的文件。目录可以使用 READ RECORD 命令读取，表 14.3 所示为 ADF 目录入口地址格式，表 14.4 所示为应用优先表明符。表中的“执行的命令”可以是 SELECT 命令的变形，通过它实现正确选择 DF，并返回文件控制信息 FCI。如果表中没有指定“执行的命令”，则需执行 SELECT 命令选择 DF。

表 14.3　ADF 目录入口地址格式

标志	长度	值						存在方式
'70'	var.	结构数据对象标签						M
		'61'	var.	应用模板				M
				'4F'	5-16	ADF 名称(AID)		M
				'50'	1-16	应用标签		M
				'9F12'	1-16	应用优先名称		O
				'87'	1	应用优先表明符(见表 14.4)		O
				'52'	var.	执行的命令		O
				'73'	var.	目录自定义模板		O
					××××	var.	一个或多个由应用提供商、发卡行或卡片供应商提供的附加(私有)数据元	O

注：“存在方式”中 M 为强制存在，O 为可选。“Var.”为变量。

3. 应用文件

与 ED/EP 应用对应的专用文件(DF)与基本数据文件构成一个树状结构的分支。该专用文件是其下属的基本数据文件的入口点。专用文件包含文件控制信息 FCI，该 DF 的上一层专用文件是主文件 MF。DF 采用应用标识符方式进行选择。

表 14.4　应用优先表明符

b_8	b_7～b_5	b_4～b_1	定义
1			需要持卡人确认方可选择应用
0			不需要持卡人确认即可选择应用
	×××		保留
		0000	未指定优先权
		××××（0000 除外）	应用的排列或选择顺序，从 1～15，其中最高优先权为 1

基本数据文件 EF 包含了应用数据，有两种类型：记录文件类型和二进制文件类型。EF 的选择是通过 READ 命令并采用短文件标识符 SFI 实现的。

表 14.5～表 14.7 列出了 3 种应用基本文件格式。

表 14.5　ED 和 EP 应用的公共应用基本数据文件

文件标识(SFI)			21(十进制)
文件类型			透明
文件大小			30B
文件存取控制		读＝自由	改写＝需要安全信息
字节	数据元		长度/B
1～8	发卡方标识		8
9	应用类型标识		1
10	应用版本		1
11～20	应用序列号		10
21～24	应用启用日期		4
25～28	应用有效日期		4
29～30	发卡方自定义 FCI 数据		2

表 14.6　ED 和 EP 应用的持卡人基本数据文件

文件标识(SFI)			22(十进制)
文件类型			透明
文件大小			39B
文件存取控制		读＝自由	改写＝需要安全信息
字节	数据元		长度/B
1	卡类型标识		1
2	本行职工标识		1
3～22	持卡人姓名		20
23～38	持卡人证件号码		16
39	持卡人证件类型		1

表 14.7　IC 卡交易明细

文件标识(SFI)		24(十进制)
文件类型		循环(至少 10 个记录)
文件存取控制		读：PIN 保护。不允许外部对其修改(由 IC 卡维护)
记录大小		23B
字节	数据元	长度/B
1～2	ED/EP 交易号	2
3～5	透支限额	3
6～9	交易金额	4
10	交易类型标识	1
11～16	终端机编号	6
17～20	交易日期(终端)	4
21～23	交易时间(终端)	3

14.2.3　EP/ED 的命令与运行状态

1. IC 卡的运行状态

在应用执行过程中，卡片总是处于以下状态之一。在某一种状态下，只能执行某些命令。

(1) 空闲状态。

(2) 圈存状态。持卡人将其在银行账户上的资金划转到 ED 或 EP 中称为“圈存”。圈存交易必须在金融终端上联机进行。

(3) 消费/取现状态。

(4) 圈提状态。持卡人将 ED 中的部分或全部资金划回到其在银行的账户上称为“圈提”。圈提必须在金融终端上联机进行。

(5) 修改状态。

应用选择完成后，卡片进入空闲状态。当卡片从终端接收到一条命令时，首先检查当前状态是否允许执行该命令。

2. 采用 ISO/IEC 7816 中定义的命令和与应用锁定相关的命令

表 14.8 中，带 * 号的是银行定义的与应用锁定相关的命令，其余的是 ISO/IEC 7816 中定义的命令。

表 14.8　命令的类别字节和指令字节

命　　令	CLA	INS	P1	P2
APPLICATION BLOCK (应用锁定)*	'84'	'1E'	'00'	'00'/'01'
APPLICATION UNBLOCK (应用解锁)*	'84'	'18'	'00'	'00'
CARD BLOCK (卡片锁定)*	'84'	'16'	'00'	'00'
EXTERNAL AUTHENTICATION (外部鉴别)	'00'	'82'	'00'	'00'

续表

命　　令	CLA	INS	P1	P2
GET RESPONSE（取响应）	'00'	'C0'	'00'	'00'
GET CHALLENGE（取口令，产生随机数）	'00'	'84'	'00'	'00'
INTERNAL AUTHENTICATION（内部鉴别）	'00'	'88'	'00'	'00'
PIN UNBLOCK（个人密码解锁）*	'84'	'24'	'00'	'00'
READ BINARY（读二进制）	'00'/'04'	'B0'	注 1	偏移地址
READ RECORD(读记录）	'00'/'04'	'B2'	记录个数	注 2
SELECT(选择）	'00'	'A4'	注 3	'00'/'02'
UPDATE BINARY（修改二进制）	'00'	'D6'	注 1	偏移地址
UPDATE RECORD（修改记录）	'00'	'DC'	记录号	注 4
VERIFY（校验）	'00'	'20'	'00'	'00'

注 1：$b_8=1$ 用 SFI 方式；$b_5 \sim b_1$ SFI 值。
注 2：$b_8 \sim b_4$ SFI 值；$b_3\ b_2\ b_1=100$，P1 为记录个数。
注 3：$b_3=1$ 通过文件名选择；否则，通过 AID 选择。
注 4：$b_8 \sim b_4$ SFI 值；$b_3\ b_2\ b_1$（$\neq 100$ 时）指定记录，$b_3\ b_2\ b_1=100$ 时由 P1 给出记录号。

与应用锁定相关命令的功能：

（1）APPLICATION BLOCK。本命令使当前选择的应用失效。P2＝00 为临时锁定应用，可解锁；P2＝01 为永久锁定。

（2）APPLICATION UNBLOCK。本命令用于恢复当前的应用。本命令完成后，由 APPLICATION BLOCK 命令产生的对应用命令响应的限制将被取消。

（3）CARD BLOCK。本命令使卡中所有应用永久失效。

（4）PIN UNBLOCK。本命令为发卡方提供了解锁个人密码的功能。

3. 为 IC 卡运行（应用规范）定义的命令

为 IC 卡运行定义的命令如表 14.9 所示。

表 14.9　为 IC 卡运行定义的命令

命　　令	CLA	INS	P1	P2
① CHANGE PIN(修改个人密码）	'80'	'5E'	'01'	'00'
② CREDIT FOR LOAD（圈存）	'80'	'52'	'00'	'00'
③ DEBIT FOR PURCHASE/CASH WITHDRAW（消费/取现）	'80'	'54'	'01'	'00'
④ DEBIT FOR UNLOAD（圈提）	'80'	'54'	'03'	'00'
⑤ GET BALANCE（读余额）	'80'	'5C'	'00'	'0X'
⑥ GET TRANSACTION PROOF（取交易认证）	'80'	'5A'	'00'	'XX'
⑦ INITIALIZE FOR CASH WITHDRAW（取现初始化）	'80'	'50'	'02'	'01'
⑧ INITIALIZE FOR LOAD（圈存初始化）	'80'	'50'	'00'	'0X'
⑨ INITIALIZE FOR PURCHASE（消费初始化）	'80'	'50'	'01'	'0X'

续表

命　　令	CLA	INS	P1	P2
⑩ INITIALIZE FOR UNLOAD(圈提初始化)	'80'	'50'	'05'	'01'
⑪ INITIALIZE FOR UPDATE(修改透支限额初始化)	'80'	'50'	'04'	'01'
⑫ RELOAD PIN(重装个人密码)	'80'	'5E'	'00'	'00'
⑬ UPDATE OVERDRAW LIMIT (修改透支限额)	'80'	'58'	'00'	'00'

现将各条命令简介如下(命令中涉及的 MAC/TAC(报文鉴别码/交易验证码)的产生使用单长度 DEA 算法,命令中讲到的密钥和计算步骤见 14.2.4 节,但输入的数据块在各交易处理流程中确定)。

① CHANGE PIN 命令。该命令允许持卡人将当前个人密码修改为新密码。该命令的数据字段为:当前 PIN ‖ 'FF' ‖ 新 PIN。以明文表示,符号 ‖ 表示链接。

② CREDIT FOR LOAD 命令。用于圈存交易,命令数据字段内容为交易日期(主机,长度为 4B)、交易时间(主机,3B)和 MAC(4B)。卡的响应数据为交易验证码(Transaction Authorization Cryptogram,TAC)(4B)。

③ DEBIT FOR PURCHASE/CASH WITHDRAW 命令。用于消费/取现交易。

命令报文数据字段内容为终端交易序号(4B)、交易日期(终端,4B)、交易时间(终端,3B)和 MAC(4B)。卡的响应数据为 TAC(4B)和 MAC(4B)。

④ DEBIT FOR UNLOAD 命令。用于圈提交易。命令数据字段内容为交易日期(主机,4B)、交易时间(主机,3B)和 MAC(4B)。卡的响应数据为 MAC(4B)。

⑤ GET BALANCE 命令。用于读取 ED/EP 余额。需验证个人密码,命令的数据字段不存在,响应的数据字段内容为余额(4B)。

⑥ GET TRANSACTION PROOF 命令。提供了一种在交易处理过程中拔出并重插卡后,卡片的恢复机制。命令的数据字段内容为要取的 MAC 和(或)TAC 所对应的当前 ED/EP 联机或脱机交易序号(2B)。响应的数据字段内容为 MAC(4B)和 TAC(4B)。

⑦ INITIALIZE FOR CASH WITHDRAW 命令。用于初始化取现交易。命令报文的数据字段内容为密钥索引号(1B)、交易金额(4B)和终端机编号(6B)。响应数据字段的内容为 ED 余额(4B)、ED 脱机交易序号(IC 卡,2B)、透支限额(3B)、密钥版本号(消费/取现子密钥,1B)、算法标识(消费/取现子密钥,1B)和伪随机数(IC 卡,4B)。

⑧ INITIALIZE FOR LOAD 命令。用于初始化圈存交易。命令的数据字段内容为密钥索引号(1B)、交易金额(4B)和终端机编号(6B)。响应的数据字段内容为 ED 或 EP 余额(4B)、ED 或 EP 联机交易序号(2B)、密钥版本号(圈存子密钥,1B)、算法标识(圈存子密钥,4B)、伪随机数(IC 卡,4B)和 MAC(4B)。

⑨ INITIALIZE FOR PURCHASE 命令。用于初始化消费交易。命令的数据字段内容为密钥索引号(1B)、交易金额(4B)和终端机编号(6B)。响应的数据字段内容为 ED 或 EP 余额(4B)、ED 或 EP 脱机交易序号(2B)、透支限额(3B)、密钥版本号(消费/取现子

密钥,1B)、算法标识(消费/取现子密钥,1B)和伪随机数(IC 卡,4B)。

⑩ INITIALIZE FOR UNLOAD 命令。用于初始化圈提交易。命令的数据字段内容为密钥索引号(1B)、交易金额(4B)和终端机编号(6B)。响应的数据字段内容为 ED 余额(4B)、ED 联机交易序号(2B)、密钥版本号(圈提子密钥,1B)、算法标识(圈提子密钥,1B)、伪随机数(IC 卡,4B)和 MAC(4B)。

⑪ INITIALIZE FOR UPDATE 命令。用于初始化修改透支限额交易。命令的数据字段内容为密钥索引号(1B)、终端机编号(6B)。响应的数据字段内容为 ED 余额(4B)、ED 联机交易序号(2B)、旧透支限额(3B)、密钥版本号(修改透支限额子密钥,1B)、算法标识(修改透支限额子密钥,1B)、伪随机数和 MAC(4B)。

⑫ RELOAD PIN 命令。用于发卡方重新给持卡人一个新的 PIN(可与原 PIN 相同)。该命令只能在拥有或能访问到重装 PIN 子密钥的发卡方终端上执行。命令的数据字段内容为重装的 PIN 值(2～6B)和 MAC(4B)。响应的数据字段不存在。

⑬ UPDATE OVERDRAW LIMIT 命令。用于修改透支限额。命令数据字段内容为新透支限额(3B)、交易日期(发卡方,4B)、交易时间(发卡方,3B)和 MAC(4B)。响应数据字段内容为 TAC(4B)。

14.2.4 EP/ED 的安全机制和密钥管理

1. 基本安全要求

为了一张卡上不同应用之间的安全,每一个应用应该放在一个独立的 ADF 中,防止跨应用的非法访问。

密钥的独立性:用于特定功能的加密/解密密钥不能被其他功能所使用,包括保存在 IC 卡中的密钥和用来产生、传输这些密钥的密钥。

IC 卡应能保证用于 RSA 算法的私有密钥或用于 DES 算法的密钥或个人密码的安全存放,在任何情况下不被泄露。

2. 安全报文传送

安全报文传送的目的是保证数据的保密性、完整性和对发送方的认证。数据的保密性通过对数据字段的加密来实现,数据的完整性和对发送方的认证通过使用报文鉴别码(Message Authentication Code,MAC)来实现。

1) MAC

在本规范中,当命令中的 CLA 字节的第 2 个半字节等于十六进制数字 4 时,表明发送方的命令要采用安全报文传送,此时将 MAC 安排在命令的数据字段的最后一个数据元位置上,MAC 的长度规定为 4B。采用 DEA 或三重 DEA 加密方法产生 MAC,步骤如下。

(1) 取 8 字节的十六进制数字 0 作为初始值。

(2) 按照顺序将以下数据连接在一起形成数据块:CLA,INS,P1,P2,Lc,数据(如果存在)。

(3) 将数据块分成 8 字节为单位的数据块,标号为 D_1、D_2、D_3 等。最后的数据块可能有 1～8 个字节。

(4) 如果最后数据块长度是 8 字节,则在其后加上 16 个十六进制数字 8000000000000000;

如果不足 8 字节,则在其后加上十六进制数字 80,加后如仍不足 8 字节,则在其后再加入十六进制数字 0,直到长度达到 8 字节。

(5) 对这些数据块使用 MAC 过程密钥进行加密。

如果采用单长度 MAC DEA 密钥,按照图 14.2 所示的过程产生 MAC;如果采用双长度 MAC DEA 密钥(KMA,KMB),则按图 14.3 所示的过程产生 MAC。

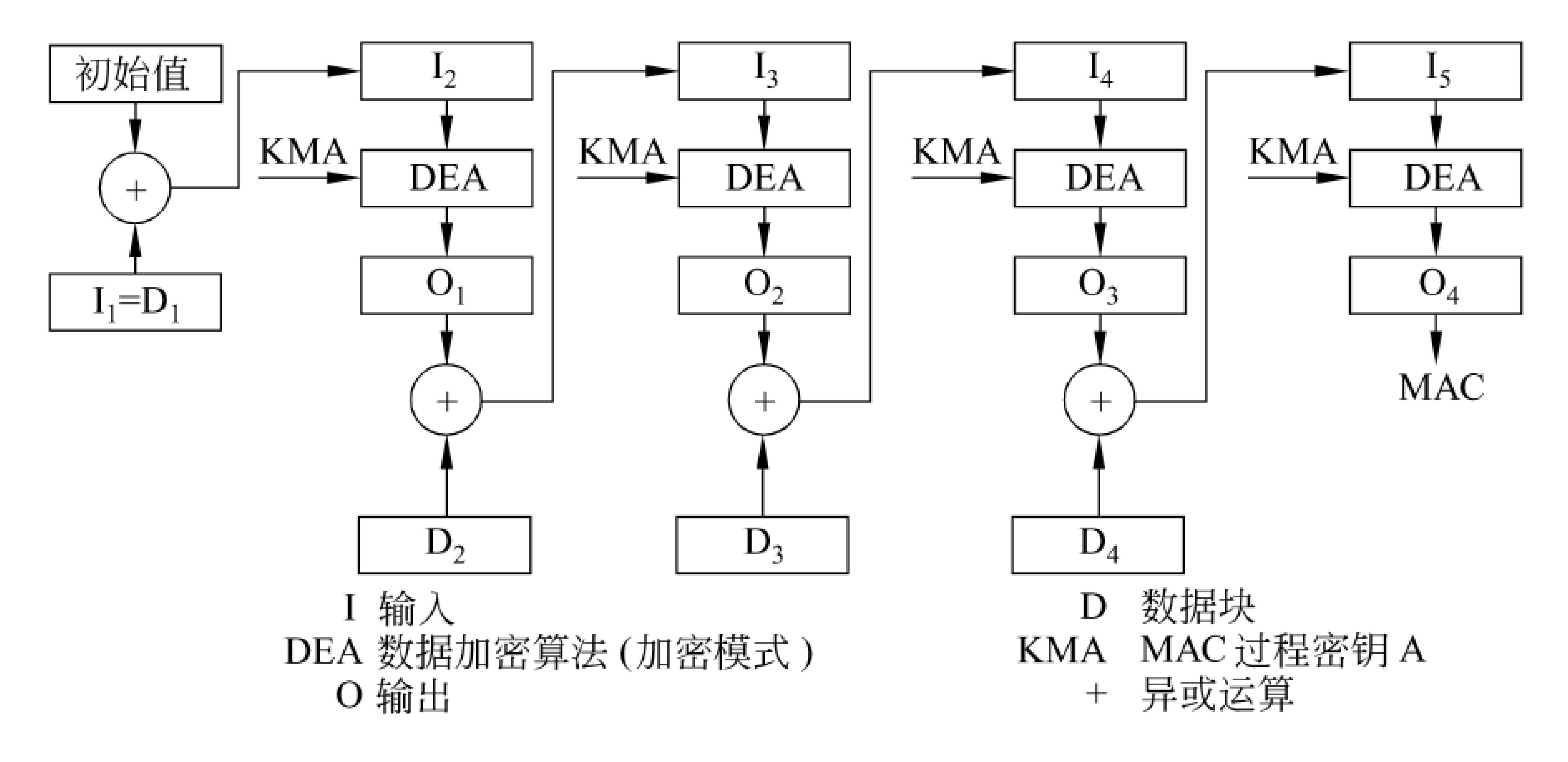


图 14.2 单长度 DEA 密钥的 MAC 算法

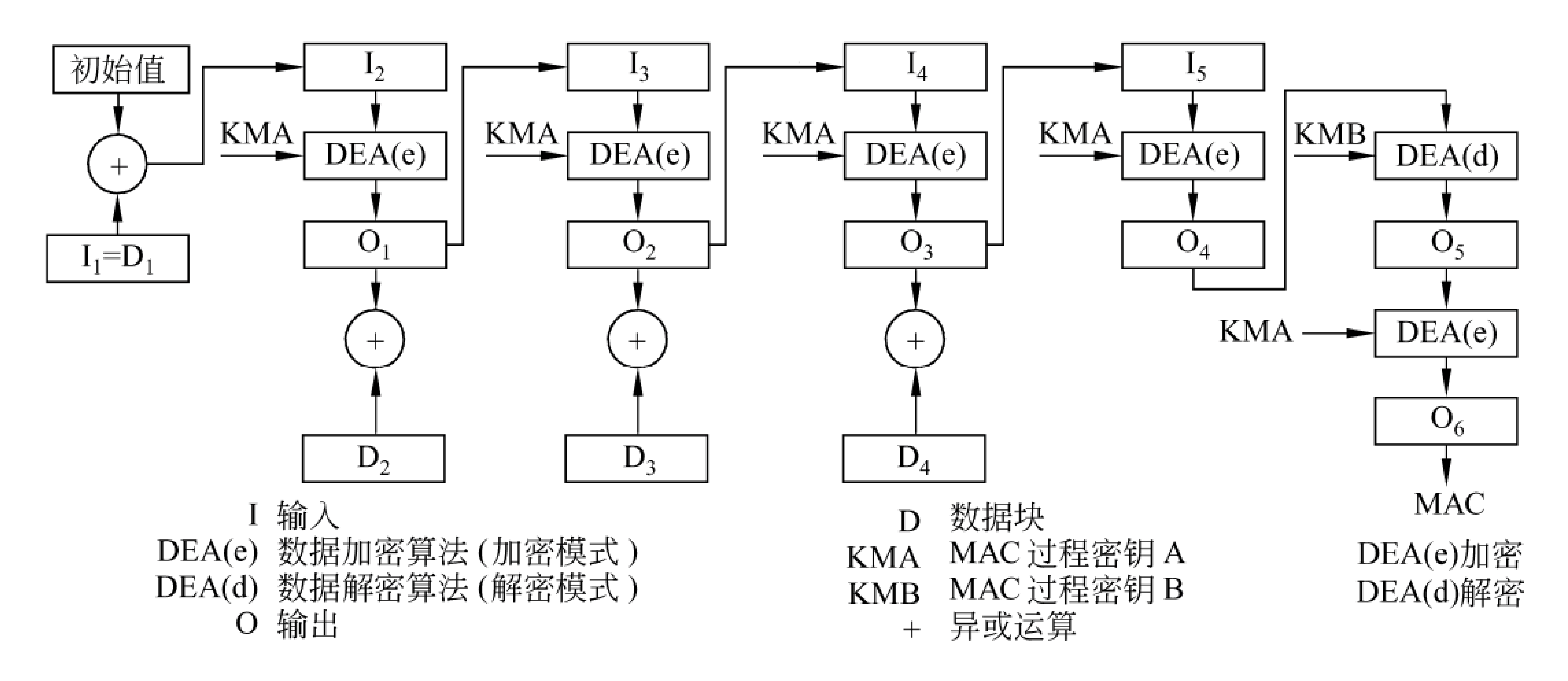


图 14.3 双长度 DEA 密钥的 MAC 算法

(6) 最终从计算结果左侧取得的 4 字节长度数据作为 MAC。

要求安全报文传送的命令,其 Lc 字段的值=数据长度+MAC 长度。即使命令不发送数据,也要发送 MAC。

2) 数据加密

数据块的形成:在明文数据的前面加上数据长度,明文数据后加上的数字与上述产生 MAC 的步骤(4)相同。整个数据块分解成 8B 数据块,标号为 D_1、D_2、D_3 等。

单长度和双长度 DEA 密钥对每一个数据块的加密过程分别如图 14.4(a)和图 14.4(b)所示,图中 KDA 为数据加密过程密钥 A,KDB 为数据加密过程密钥 B,其余

的解释同图 14.3。

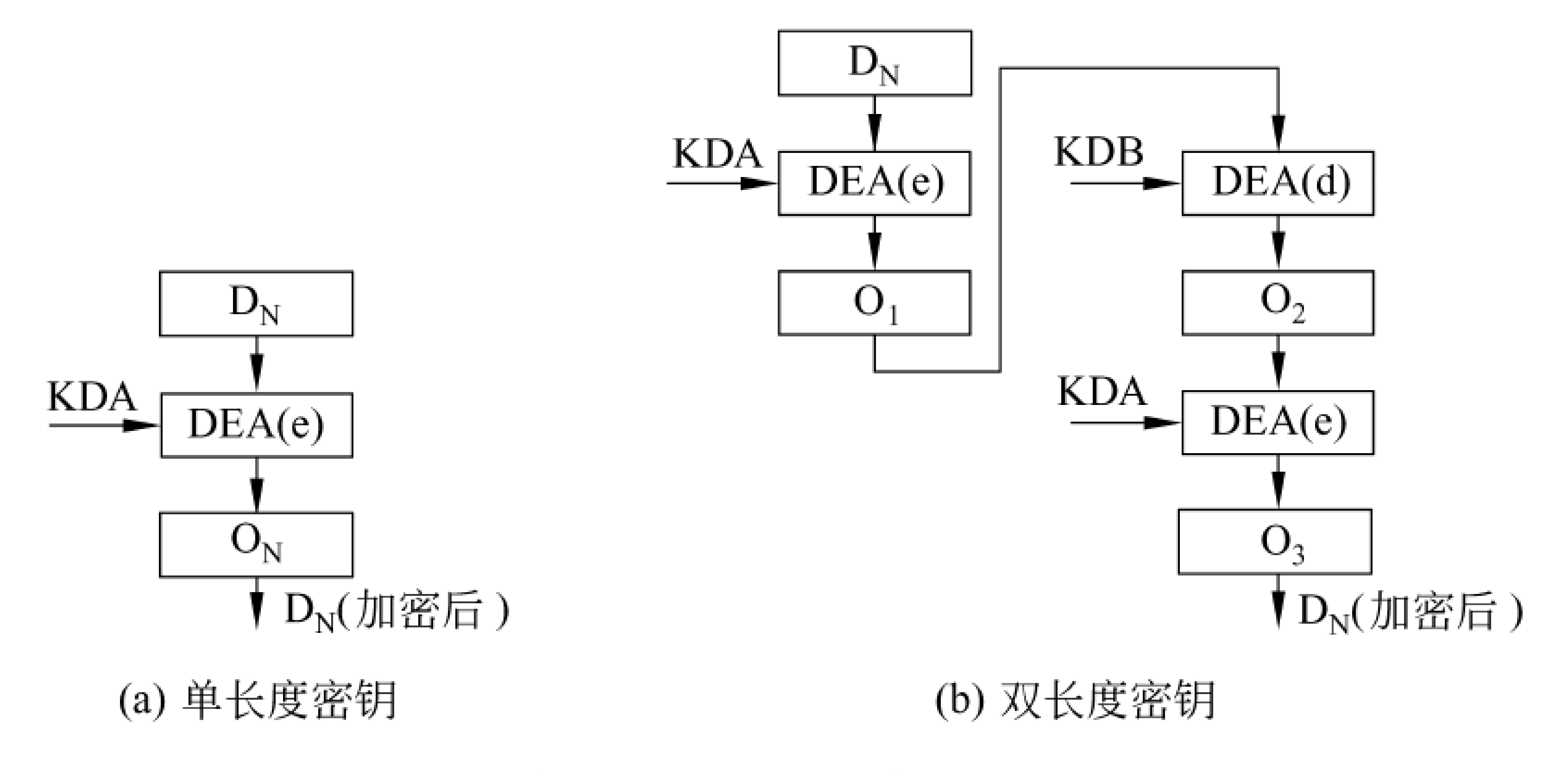


图 14.4 单/双长度 DEA 密钥对数据加密过程

3）数据解密

步骤与数据加密相同，但将图 14.4 中的加密操作改为解密操作；解密操作改为加密操作。

3. 认可的加密算法（参见第 5 章）

（1）对称算法（DES）。

（2）非对称算法（RSA）。

（3）安全哈希算法（SHA-1）。输入任意长度信息，产生一个 160 位的哈希值。SHA-1 的标准见 ISO/IEC 10118-3。

4. 密钥管理

涉及资金划转或修改 IC 卡中敏感数据的交易，必须使用加密密钥来保证应用的安全。

金融 IC 卡的密钥采用集中（或部分集中）管理方式，即发卡单位（总行）将密钥分发给所辖发卡方。

1）密钥的 3 个层次

密钥分为 3 个层次：主密钥—子密钥—过程密钥。分别以 M、D 和 SES 作为起始字符。

ED/EP 应用中的主密钥有消费/取现主密钥 MPK，圈存主密钥 MLK，TAC 主密钥 MTK，PIN 解锁主密钥 MPUK，重装 PIN 主密钥 MRPK，应用维护主密钥 MAMK，圈提主密钥 MULK 和更新主密钥 MUK。相应的子密钥有 DPK、DLK、DTK 等。

IC 卡收到初始化命令后，使用命令中给出的密钥索引号找到卡中相应密钥进行运算。

过程密钥（SESsion）只用于交易的特定阶段，相应的过程密钥有 SESPK、SESLK、SESDTK 等。IC 卡上的密钥必须安全存储。

2）子密钥推导方法

本节描述了 IC 卡中密钥的推导方法。图 14.5 和图 14.6 所示为消费/取现子密钥 DPK 推导的过程。

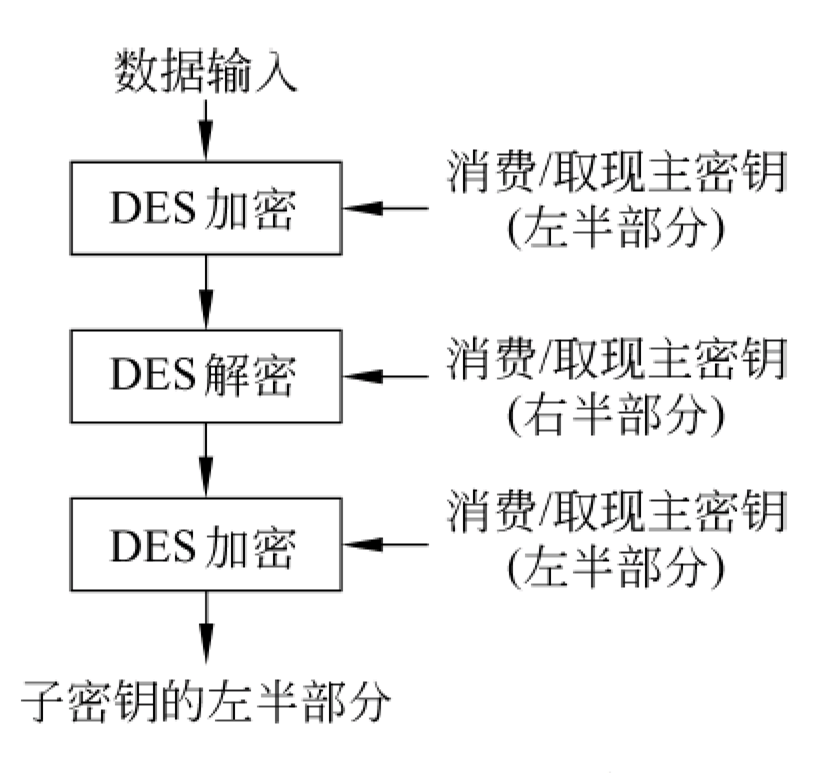


图 14.5　推导消费/取现子密钥左半部分

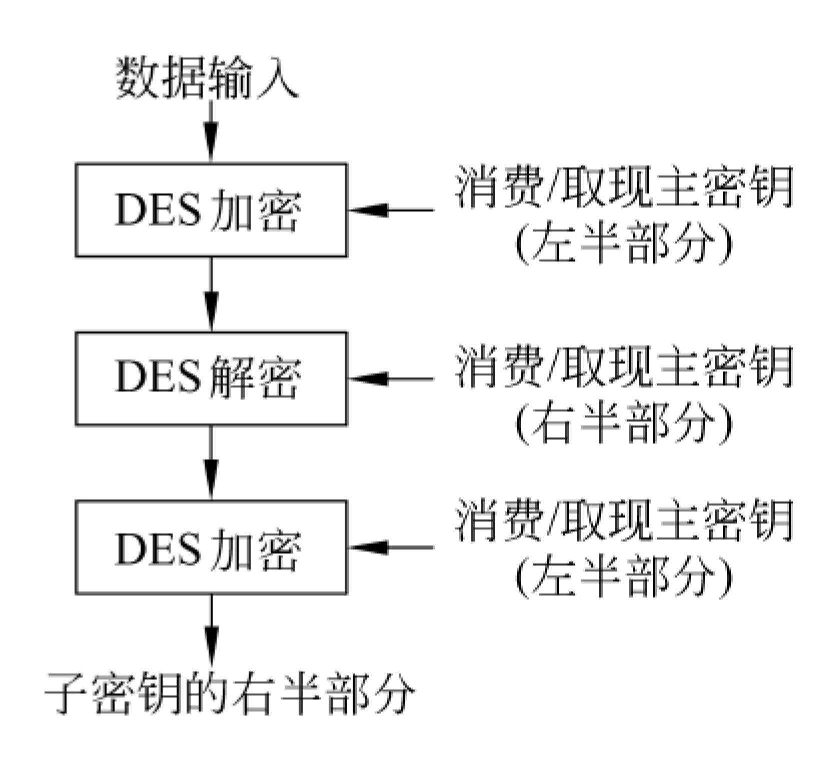


图 14.6　推导消费/取现子密钥右半部分

(1) 子密钥左半部分的推导方法。推导双倍长子密钥左半部分的方法如下。

① 将应用序列号的最右 16 个数字作为输入数据。

② 将消费/取现主密钥作为加密密钥。

③ 用消费/取现主密钥对输入数据进行 3DEA 运算。

(2) 子密钥右半部分的推导方法。推导双倍长子密钥右半部分的方法如下。

① 将应用序列号的最右 16 个数字的求反作为输入数据。

② 将消费/取现主密钥作为加密密钥。

③ 用消费/取现主密钥对输入数据进行 3DEA 运算。

图 14.5 和图 14.6 所示的方法同样适用于 ED 的消费/取现、圈存和圈提、修改等子密钥的推导及 EP 的消费和圈存子密钥的推导。

3) 过程密钥

过程密钥是在交易过程中用可变数据产生的单倍长密钥。交易类型不同,产生过程密钥的输入数据和密钥也不同。

过程密钥产生后只能在某过程/交易中使用一次。

图 14.7 所示为 EP 进行消费/取现时产生过程密钥的机制。此方法也用于不同交易类型的过程密钥的产生,但输入的数据取决于不同的交易类型。

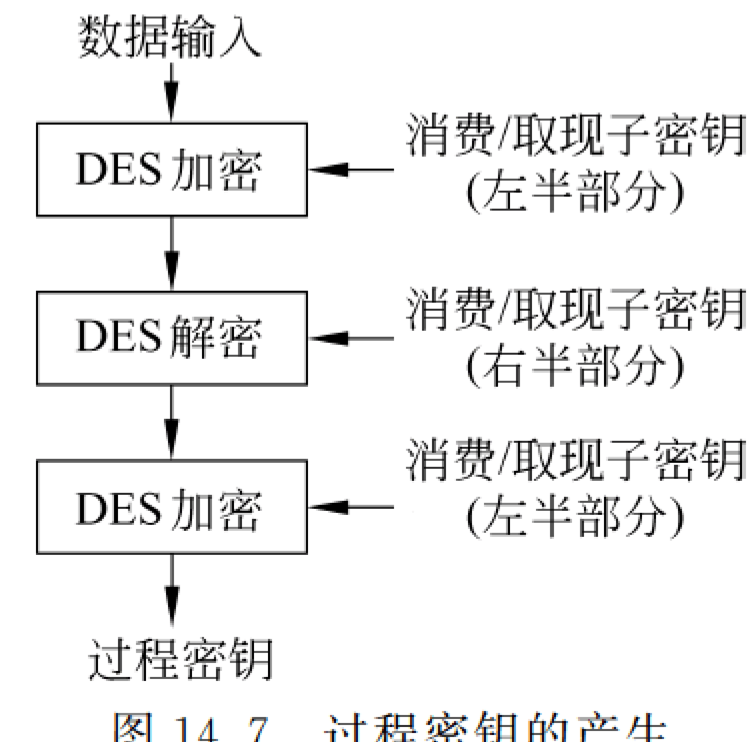


图 14.7　过程密钥的产生

5. 终端

终端应该支持用来输入个人密码的键盘。应该是可以在有人或无人管理环境中运行的联机/脱机终端。

14.2.5　EP/ED 的交易流程

消费或取现要求终端必须具有安全存取模块(Purchase Secure Access Module, PSAM)。

1. 交易预处理

图 14.8 所示为对电子存折/电子钱包的共有预处理流程。

步骤说明如下。

(1) 插入 IC 卡。

(2) 应用选择。应用标识符由全国金融标准化技术委员会负责分配和维护。成功地选择了 ED/EP 应用后,IC 卡回送 FCI。表 14.7 定义了此应用必备的 FCI 发卡方专用数据(表中的"数据元")。

(3) IC 卡有效性检查。对于 SELECT 命令回送的数据,终端进行以下检查:卡是否在黑名单上;终端是否支持发卡方标识符、应用类型和应用版本;应用是否在有效期内。

(4) 错误处理。当有效性检查有任一条件不满足时,进行错误处理。

(5) 选择 ED 或 EP。

(6) 输入 PIN(仅 ED 或 EP 圈存需要)。

(7) 检验 PIN(仅 ED 或 EP 圈存需要)。如果输入错误的 PIN 超过指定的次数,则终止交易。否则再一次输入 PIN。

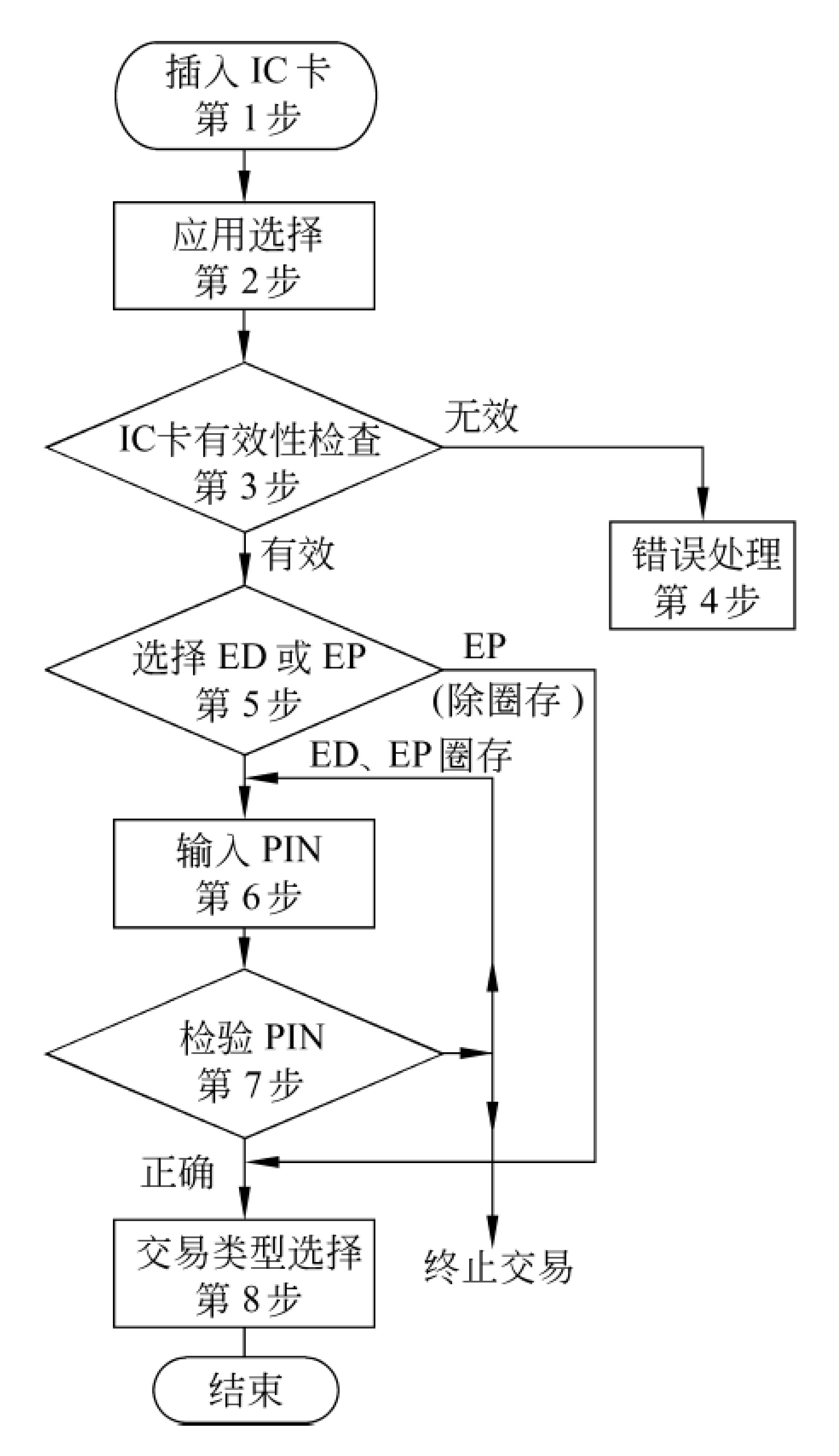


图 14.8 交易预处理流程

(8) 交易类型选择。让持卡人选择交易类型,每次选择一种。对于 ED,持卡人能选择的交易为圈存、圈提、消费、取现、查余额和查明细等。对于 EP,持卡人能选择的交易为圈存、消费和查余额。

2. 圈存交易

通过圈存交易,持卡人可将银行账户上的资金划入 ED/EP。这种要求必须在金融终端上联机进行并提交 PIN。

交易步骤如图 14.9 所示。

(1) 终端发出 INITIALIZE FOR LOAD 命令。

(2) IC 卡处理命令,进行以下操作。

① 检查卡是否支持命令中的密钥索引号。

② 产生一个伪随机数,过程密钥和报文鉴别码 MAC1,用以供主机验证圈存交易和 IC 卡的合法性。

过程密钥是用子密钥产生的。产生过程密钥的输入数据如下。

- 伪随机数 ‖ ED/EP 联机交易序号 ‖ '8000'。
- 用过程密钥对以下数据加密产生 MAC1:ED 或 EP 余额、交易金额、交易类型标

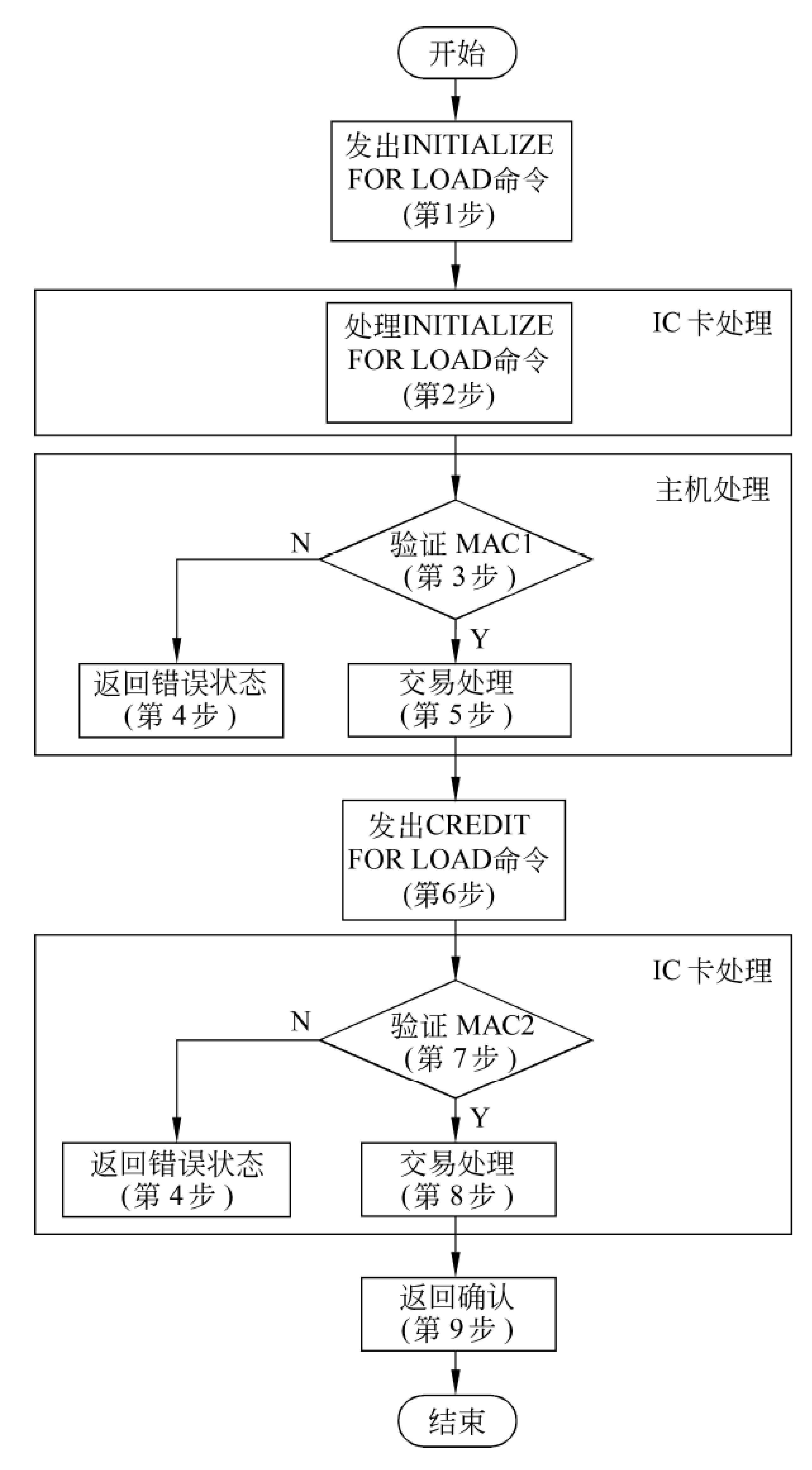


图 14.9　圈存交易处理流程

识和终端机编号。

(3) 验证 MAC1。收到 INITIALIZE FOR LOAD 响应后,主机产生过程密钥并确认 MAC1 是否有效。

(4) 回送错误状态。如果不接受圈存交易,主机回送错误状态给终端。

(5) 交易处理。在确认可进行圈存交易后,主机从持卡人在银行账户中扣减圈存金额。

主机产生一个报文鉴别码 MAC2,用于 IC 卡对主机合法性进行检查,用以下数据加密产生 MAC2:交易金额、交易类型标识、终端机编号、交易日期(主机)和交易时间(主机)。

主机将 ED/EP 交易序号加 1,并向终端发送圈存交易接受报文,其中包括 MAC2、交

易日期（主机）和交易时间（主机）。

（6）终端发出 CREDIT FOR LOAD 命令。

（7）验证 MAC2。IC 卡验证 MAC2 有效性，如果无效返回第 4 步。

（8）交易处理。IC 卡将 ED/EP 联机交易序号加 1，并将交易金额加到余额上。

在圈存交易中，IC 卡用以下数据组成一个记录更新交易明细：ED/EP 联机交易序号、交易金额、交易类型标识、终端机编号、交易日期（主机）和交易时间（主机）。

产生交易验证码，TAC 的计算不采用过程密钥方式，而是用子密钥左右 8B 的异或运算结果对以下数据进行加密运算来产生：ED/EP 余额、DE/EP 联机交易序号（加1 前）、交易金融，交易类型标识、终端机编号、交易日期（主机）和交易时间（主机）。

（9）返回确认。IC 卡通过 CREDIT FOR LOAD 命令的响应将 TAC 回送给终端。主机可以不马上验证 TAC。

3. 圈提交易

持卡人将 ED 中部分或全部资金划回到银行账户上。这种交易必须在金融终端上联机进行，并提交 PIN。圈提交易的流程如图 14.10 所示。

操作步骤中，第 1～7 步基本上与圈存交易相似，除了密钥不同外，在第 5 步时还不能更改主机账户上的金额。

下面从第 8 步开始解释。

第 8 步交易处理。IC 卡将 ED 联机交易序号加 1，并从卡上余额中减去交易金额。

IC 卡产生报文鉴别码 MAC3，并通过 DEBIT FOR UNLOAD 命令的响应报文，将以下数据经终端送主机：电子存折余额、DE 联机交易序号（加 1 前），交易金额、交易类型标识、终端机编号、交易日期（主机）和交易时间（主机）。

IC 卡用以下数据组成一个记录更新交易明细：ED 联机交易序号、交易金额、交易类型标识、终端机编号、交易日期（主机）和交易时间（主机）。

第 9 步验证 MAC3。主机收到 MAC3 之后，验证其是否有效。如无效，返回第 4 步。

第 10 步交易处理。发卡方主机将交易金额加到持卡人银行账户上，并将主机的联机交易序号加 1。主机将向终端回送一个报文（报文内容本规范不作规定）。

第 11 步显示完成。终端向持卡人显示交易完成信息，如果需要，终端应向持卡人提供交易纸凭证。

4. 消费交易

持卡人使用 ED/EP 的余额进行购物或获取服务，此交易可在销售点终点上脱机进行。使用 ED 进行消费需提交 PIN，使用 EP 则不需要。

消费交易处理流程如图 14.11 所示。

对此流程不做详细解释，仅简单说明如下。

（1）终端内设置 PSAM 模块，利用它产生过程密钥和报文认证码 MAC。

（2）在 IC 卡上扣款是在第 6 步执行的。同时产生 MAC2。

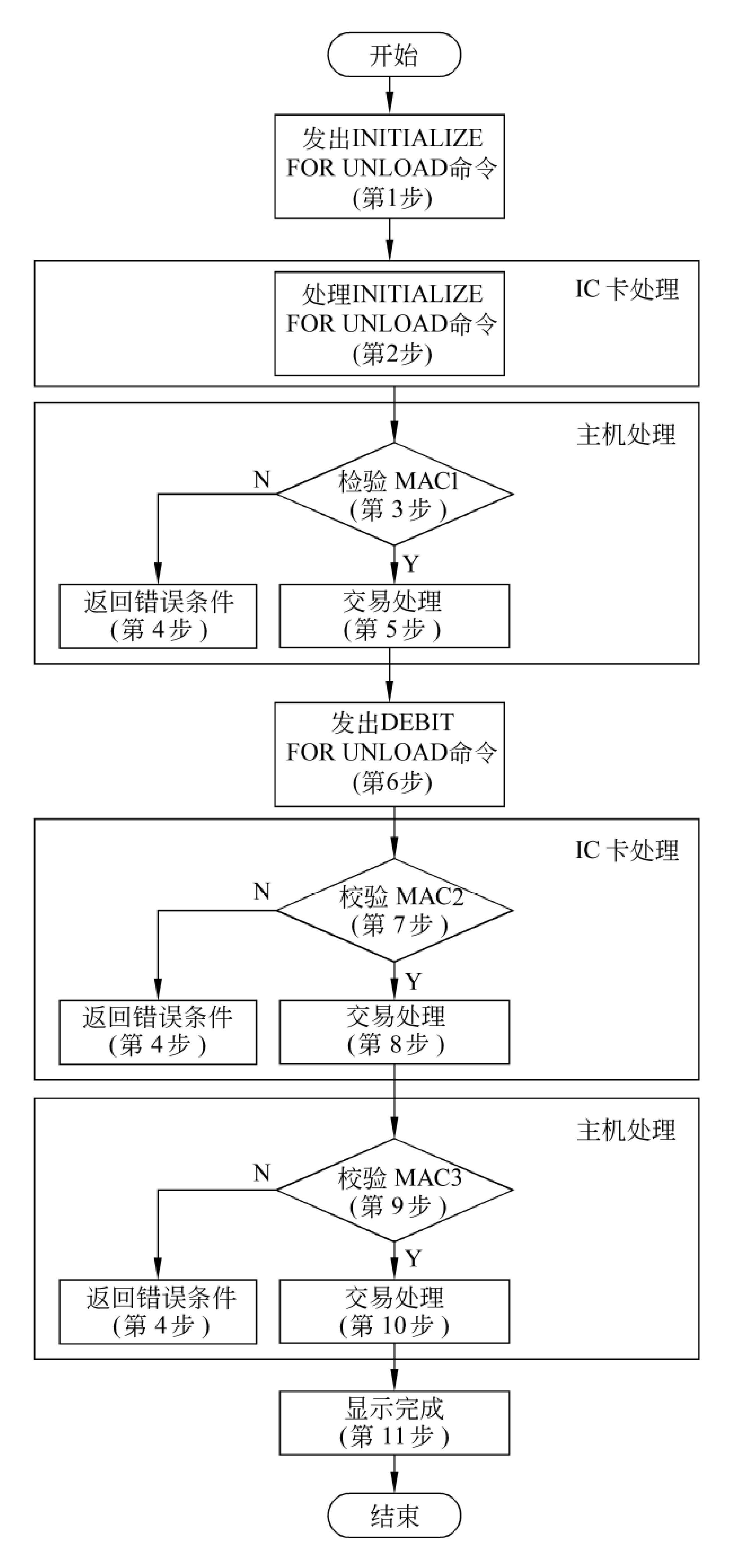


图 14.10　圈提交易处理流程

(3) 在第 7 步,PSAM 要验证 MAC2 的有效性。MAC2 的验证结果被送到终端,以便采取必要的措施,终端采取的措施不在本规范中规定。

5. 取现交易

持卡人从 ED 中提取现金,必须提供 PIN。

操作流程及其说明见中国金融集成电路(IC)卡规范。

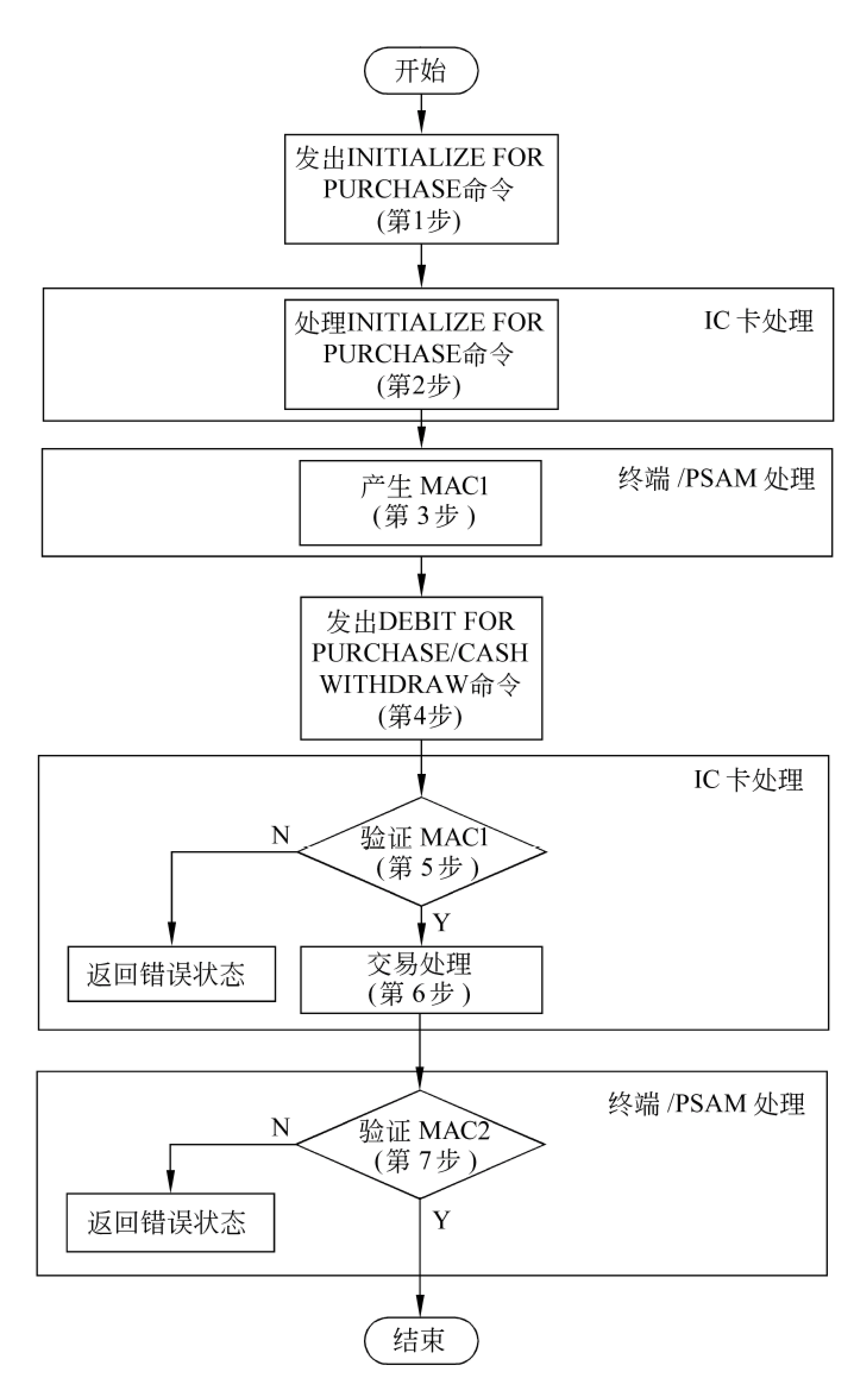


图 14.11　消费交易处理流程

6. 修改透支限额交易

当电子存折中的实际金额不足时，它为持卡人提供了一种在发卡方所允许的透支额度内继续进行交易的方便性。修改透支限额必须在金融终端上联机进行，且须提交 PIN。

是否允许透支及透支额度由发卡方决定。如果透支限额存在，电子存折的余额实际上是圈存余额和透支限额之和。

本交易的操作流程及其说明，见中国金融集成电路(IC)卡规范。

7. 查询余额交易

终端利用 GET BALANCE 命令查询余额。

8. 查询明细交易

查询明细交易一般采用脱机方式处理，需提交 PIN。

终端发 READ RECORD 命令来获得交易明细。回送某个交易明细记录中所含的所有数据。交易明细文件为循环记录文件,至少应包含 10 条记录。使用记录号寻址,记录号从 1 到 n,n 是文件中记录的最大个数。最近写入的记录号为 1,前一记录号为 2,依次类推到 n。

9. 防拔

卡片必须在交易中的任何情况下,甚至在更新 E^2PROM 过程中掉电的情况下,保持数据的完整性。这需要在每次更新数据前对数据进行备份,并且在重新加电后自动恢复数据。

14.2.6 中国金融卡规范与移动支付

1. PBOC 规范和 EMV 标准

2013 年 2 月推出 PBOC 3.0 规范,对小额非接触支持应用功能加以扩充和完善,支持双币电子现金支付应用(双币:人民币和国际货币),规范了 IC 卡和互联网终端技术要求,丰富了安全算法体系。

在国际上,EMV 标准是公认的全球统一标准,是由国际三大银行卡组织 Europay(欧陆卡,已被万事达收购)、Master Card(万事达卡)和 VISA(维萨)共同制定的银行卡技术标准,大大提高银行卡的支付安全性,截至 2014 年正式发布的版本有 EMV96 和 EMV2000。

EMV2000 标准的主要内容是借记/贷记应用交易流程、借记/贷记应用规范和安全认证机制等。1999 年 2 月,当时的三大银行卡组织共同成立了 EMVCO 组织。

EMV 迁移是按照 MV2000 标准,将银行卡从磁卡迁移成 IC 卡。这是必然的趋势。

我国的国家商用密码管理办公室发布了 SM 系列算法,并建立了国产密码产品安全检测认证体系。PBOC 中国密码算法与国际算法的对应关系如表 14.10 所示。

表 14.10 PBOC 中国密码算法与国际算法的对应关系

PBOC 2.0 及 EMVCO 规范算法	PBOC 3.0 国际 SM 算法
RSA	SM2
SHA-1	SM3
3DES	SM4

2. 移动支付(Mobile Payment)

(1) 使用手机,通过移动通信网络对账户进行查询、转账或购物消费,是移动通信技术、无线射频技术、互联网技术相互融合的结果。移动支付业务由移动运营商、移动应用服务提供商和金融机构(银行、第三方)共同实现,为用户建立一个与手机号码关联的支付账户。当前第三方移动支付市场有支付宝、微信手机支付、百度钱包等。

实现以上条件要求具有能联网的移动终端、移动运营商提供的网络服务、银行提供的

线上支付服务、移动支付平台和商户提供的商品或服务。

(2) 虚拟卡交易。一个手机 APP,配以 HCE(Host-based card Emulation,基于主机的卡模拟)软件,即可扮演成一个智能卡,是一个虚拟的模拟智能卡。但是 HCE 内没有 SE(安全元件),因此降低了安全性,于是出现了各种技术以提高安全性。

(3) 闪付(Quick Pass)。具有“闪付”功能的金融卡或银联的移动支付产品,在支持银联“闪付”非接触式支付终端上(POS 机),轻松一“挥”便可快速完成支付单笔金额(小额),无须输入密码和签名。接收支付的商户包括超市、百货、药房、快餐连锁和加油站、停车场、旅游景点等服务领域。

销售点(Point Of Sales, POS)对商品交易提供数据服务的非现金结算,是一种多功能终端。它安放在特约商户和受理网点中,与计算机联成网络,实现电子资金自动转账,具有支持消费、预授权、余额查询和转账等功能。

(4) 2015 年 12 月,中国银联分别与手机制造企业苹果公司、三星公司宣布合作,在中国推出移动支付手机,中国银联推出“云闪付”。

“云闪付”采用 NFC、HCE、Token 等国际主流的支付技术,需要采用有 NFC 功能的手机和安卓操作系统,以及与具有银联“闪付”标识兼容的 POS 机实现小额、非接触快捷支付功能。另外三星、华为、中兴等公司也推出了类似产品。

苹果手机采用 NFC 技术,手机内嵌入安全元件(SE)、指纹识别、无须运行手机 APP,但在 iPhone 6 以上的手机才能使用。

NFC(Near Field Communication)采用近距离无线通信技术,工作于 13.56MHz 和 10cm 范围内,从 RFID 演变而来,由飞利浦半导体(现在的恩智浦半导体公司)、诺基亚和索尼公司共同研制开发。

Token 用于身份验证,有些地方将它翻译成令牌。

金融卡和手机都可认为是智能终端,与“人、物”接触,在互联网与物联网基础上为人们提供服务。但是诈骗手段也会升级,例如非法基站、欺骗电话等。

14.3 RFID 的应用

RFID 在各行各业中的应用促成了物联网技术的发展,将信息技术与各个行业、多门学科进一步结合,以提高生产力,改善生产条件和生态环境,支持经济和社会的发展。

14.3.1 一位系统

一位可以有两种状态:1 或 0。用一位来表示读写器作用范围内有电子标签或没有电子标签,其典型应用就是商场中某些商品贴上电子标签,供收款时监视。

一般由读写器、电子标签和去活化器几部分组成,去活化器可以在商品付款后使电子标签去活化,变得无效。在某些系统中,去活化后的电子标签可以重新活化,成为可以再次使用的电子标签。

14.3.2 RFID在生产流水线中的应用

下面介绍的系统采用RFID技术作为制造业生产流水线现场制品跟踪和生产状态监控的基础,实现了制造和质量的可视化和数字化管理。

系统的总体结构如下。

1. 系统构成

基于RFID的执行制造系统(Manufacturing Execution System, MES)如图14.12所示。车间控制器位于企业上层管理层和车间控制层之间,实现现场控制系统与上层的企业资源计划(Enterprise Resource Planning,ERP)系统等部门的联系,实现生产的管理和数据的传送。

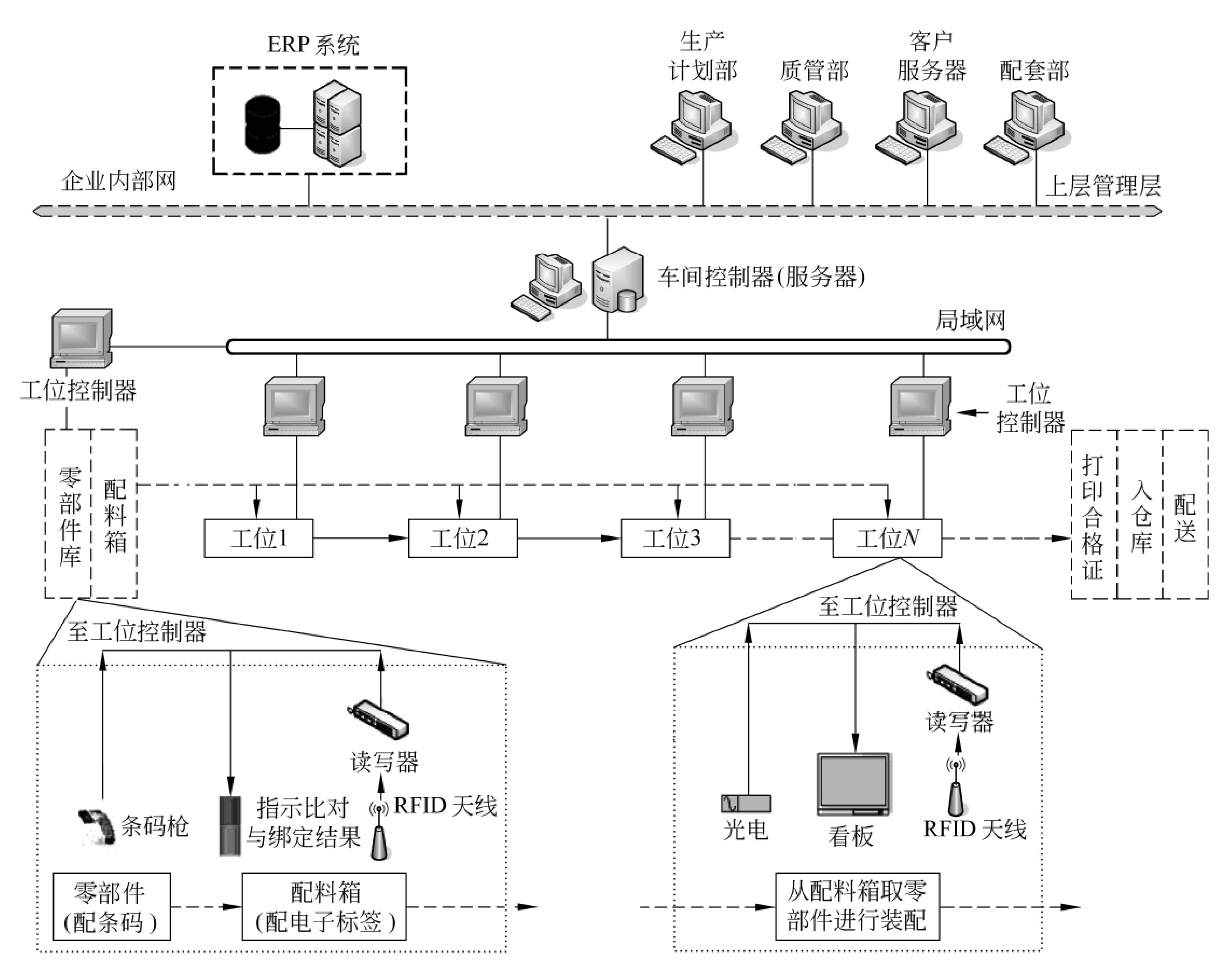


图14.12 基于RFID的MES系统构成

底层工位控制器下连生产线上各种生产控制和检测设备,上接车间控制器,实现底层生产数据的采集及其与车间控制器的通信。一般置于生产线关键工位处。

2. 工位典型配置

关键工位设有工位控制器,工位控制器下连RFID读写器、电子看板等生产控制和检测设备,上接车间控制器,实现工位生产数据的采集及其与车间控制器的通信和应用集

成。工位典型配置如图 14.13 所示。

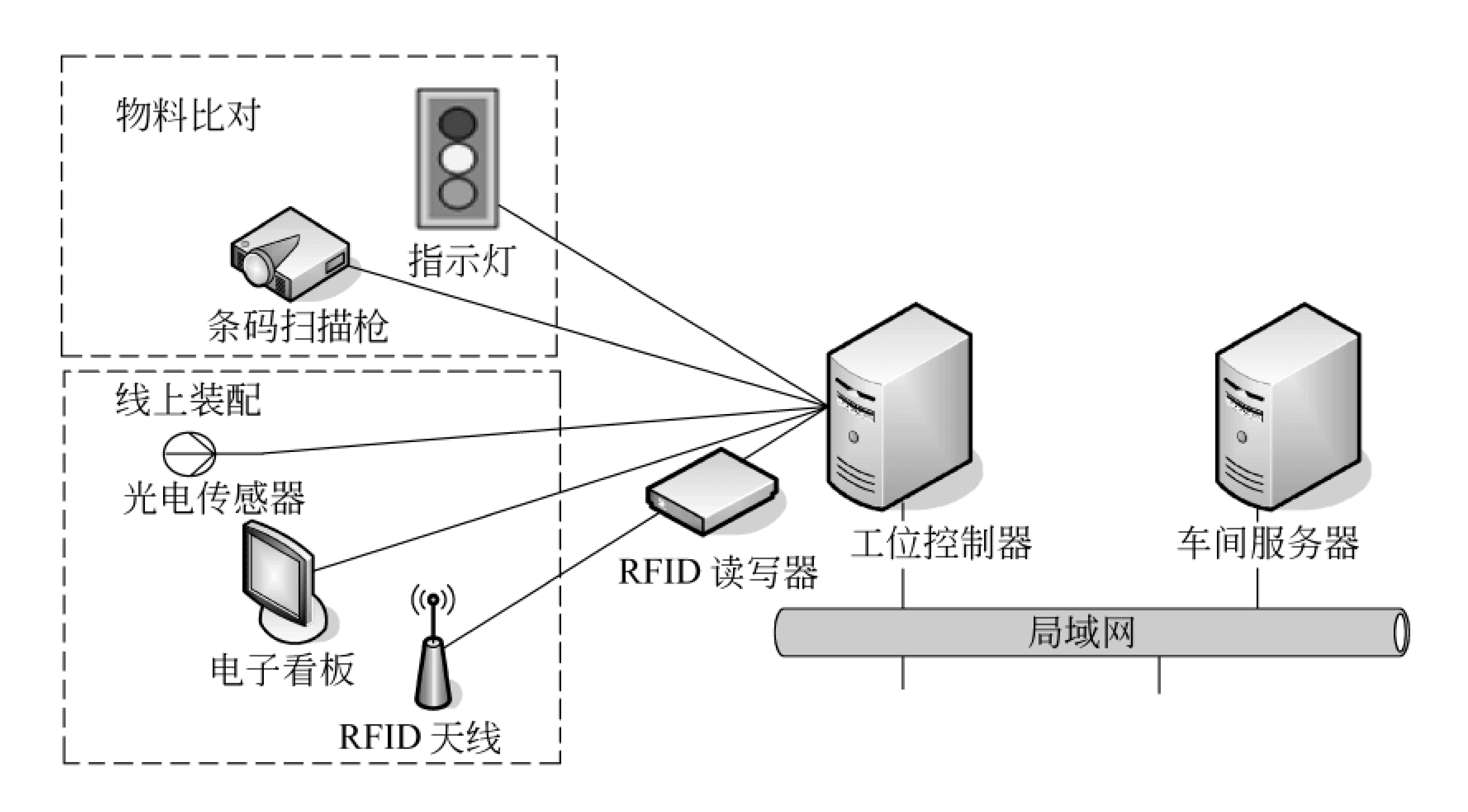


图 14.13　工位典型配置

14.3.3　RFID 在井下人员跟踪管理中的应用

1. 概述

为了减少煤矿井下作业的安全事故，加强下井人员管理成为煤矿安全工作的一个重要环节。将 RFID 技术应用于煤矿井下人员的跟踪和管理，可实现井下人员行踪的实时反映和自动记录，在地面主控计算机及局域网中均可查阅当前井下各区段、各采区的员工人数分布及人员信息，能加强对煤矿井下人员的安全管理，有助于提高安全生产效率，有利于控制安全隐患和进行抢险救灾工作。

2. 系统架构

利用 RFID 技术的优势，建立一个能对井下流动工作人员进行定位、跟踪，并通过基站实现地面控制管理中心与井下员工通信的安全管理系统。系统由井上与井下两部分设备组成。井上设备主要由前端监控中心构成，监控中心由前端服务器、后台服务器、后台数据库等组成，前端服务器中设置有能反映井下情况的显示大屏幕；井下设备由分布在各巷道监测点的监控分机、RFID 读写器、信息发送设备及下井人员携带的 RFID 卡构成。系统框架如图 14.14 所示。

考虑到煤矿井下的复杂环境和布线的难度，所以本系统在每一个巷道的交叉口及必要监测点安装监控分机，每个分机可以同时连接多个 RFID 读写器，分机与 RFID 读写器之间通过无线的方式进行数据传输，读写器和分机的安装距离要求小于 30m。前端服务器通过通信交换机与井下各监控分机连接，前端服务器与后台数据库服务器的距离较远，采用稳定性好、传输距离远的以太网。

下井人员按照要求佩戴安装电子标签的腰带，或者佩戴装有电子标签的安全帽，电子标签中存储表明员工身份的识别号，各分机及读写器都被指定了代表安装位置的识别号。RFID 读写器通过固定频率的射频载波向电子标签传送信号，当井下人员经过读写器射频场时，人员电子标签被激活并将载有人员身份信息的射频信号读取出来。RFID 读写

器读取出的人员身份信息经信息发送装置发射至监控分机。RFID 读写器、监控分机提供的位置信息与人员电子标签提供的身份信息及分机内的时间信息进行组合,形成跟踪和管理系统的基础信息,通过通信线路送往地面的前端服务器。该基础信息在系统软件的控制下生成并记录井下人员所在位置、到达时间和活动轨迹等实时跟踪信息,并可自动生成考勤的统计管理等方面的报表资料。

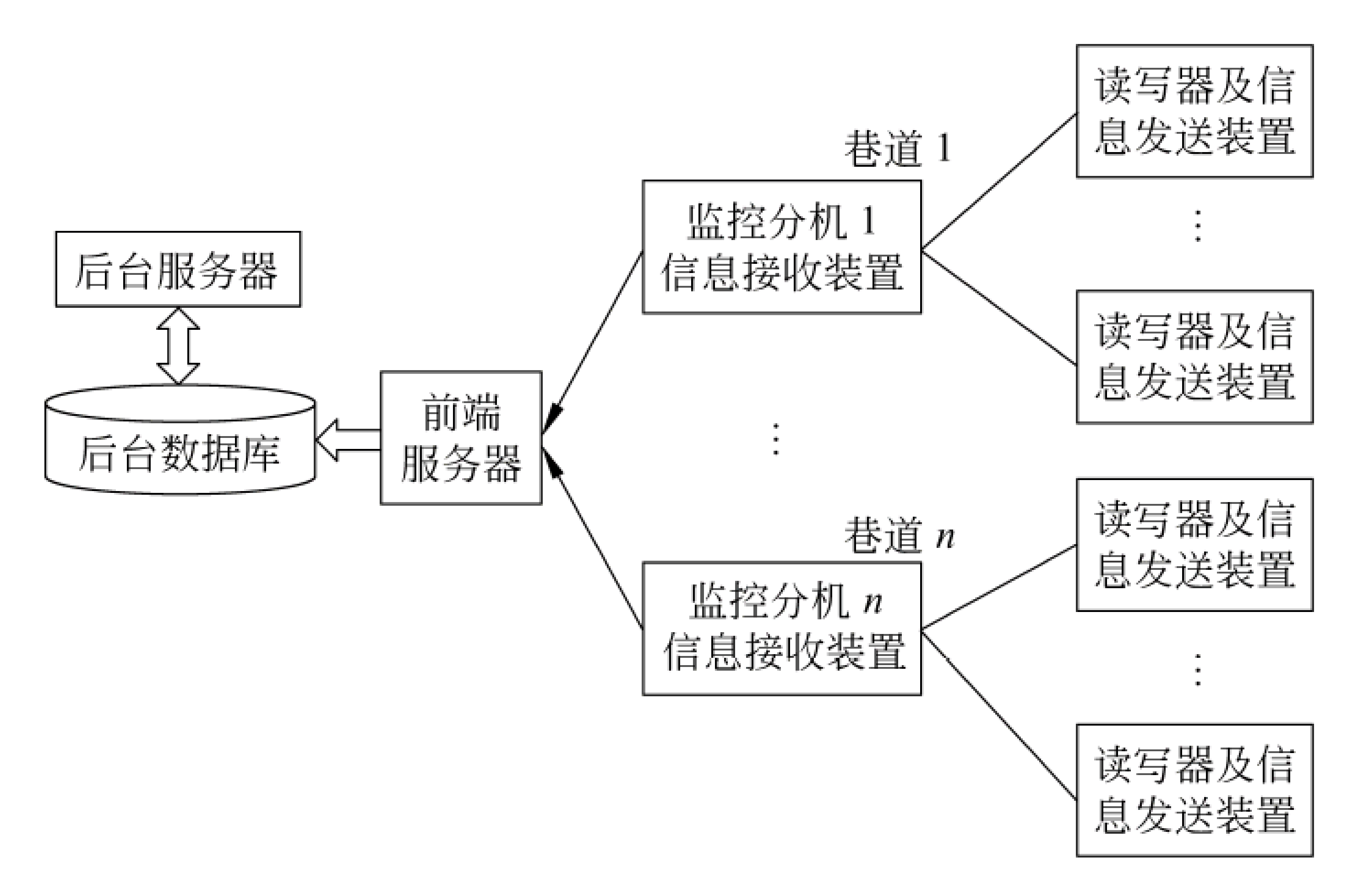


图 14.14　系统框架

3. 系统硬件设计

系统硬件主要包括 RFID 读写器发送装置、监控分机中的信息接收装置和前端服务器等。信息接收装置由具有串口通信功能的最小单片机系统和多个无线接收装置组成。前端服务器由具有以太网接口的系统担当。监控分机接收并暂存来自多个读写器的身份识别数据,经过分机主控单片机的处理和数据压缩后按照与地面主机约定的通信协议发往地面主机。分机主控单片机进行的数据处理包括冗余数据剔除、数据标识和行进方向判断等。

监控分机可以独立工作,当地面主机或通信系统发生故障时各井下分机仍可控制所属的读写器正常工作,获得的基本数据暂时保存在分机数据库内待故障排除后补充到地面主机中。监控分机内带有后备电源,当交流电源停电时由后备电源供电。后备电源由可充电电池及相应的电源管理电路组成。

4. 系统软件功能设计

系统软件由主控模块、井下监控分机与地面主机通信模块、后台数据库系统、动态绘图模块及局域网络构成,完成以下主要功能。

(1) 查询当前井下人员分布。根据各矿井实际情况绘制井下巷道布置图,并在该图上显示各个区域当前人数和井下人员移动情况。

(2) 井下人员跟踪。为不同工种的人员指定不同符号,在井下巷道图上实时动态地显示他们的行踪。

(3) 安全保障功能。一旦出现矿井灾难,可对现场被困人员进行定位和搜寻,便于有效救护。

（4）考勤管理功能。

（5）生产调度功能。

（6）网络功能。网络软件安装在煤矿管理中心的服务器中，所有合法用户均可在联网计算机中通过浏览器实时调阅本系统内容，实现远程管理。

5. RFID技术在井下人员跟踪管理系统的适应性分析

RFID技术应用于井下人员安全管理系统具有如下突出优点。

（1）快速扫描。RFID读取器可同时辨识和读取数个RFID标签，提高下井人员信息的采集效率。

（2）体积小型化、形状多样化。RFID在读取上并不受尺寸大小与形状限制，易于向小型化发展，便于携带。

（3）抗污染能力和耐久性。RFID对水、油和化学药品等物质具有很强抵抗性，RFID标签将数据存在芯片中，可以免受污损，利于长期使用。

（4）穿透性和无屏障阅读。RFID能够穿透非金属或非透明的材质，便于在井下有阻隔的恶劣环境下通信。

（5）数据记忆容量大。能够满足对人员姓名、身份证号和工种等多种信息的存储需求。

（6）易于与IT、计算机网络和GIS、GPS技术集成，构建现代化信息管理系统。

14.3.4 RFID在供应链管理中的应用

1. 概述

RFID技术，作为快速、实时、准确采集与处理信息的高新技术和信息标准化的基础，免除了标签识读过程中的人工干预，在节省大量人力的同时可极大地提高工作效率和数据的准确程度，所以RFID技术对物流和供应链管理具有巨大的吸引力。从采购、存储、生产制造、包装、装卸、运输、流通加工、配送、销售到服务，是供应链上环环相扣的业务环节和流程。在供应链运作时，企业必须实时地、精确地掌握整个供应链上的商流、物流、信息流和资金流的流向和变化，使这4种流及各个环节、各个流程都协调一致、相互配合，才能发挥其最大经济效益和社会效益。然而，由于实际物体的移动过程中各个环节都是处于运动和松散的状态，信息和方向常常随实际活动在空间和时间上变化，影响了信息的可获性和共享性。而RFID正是有效解决供应链上各项业务运作数据的输入输出、业务过程的控制与跟踪，以及减少出错率等难题的一种新技术。

2. RFID技术在供应链各环节中的应用

1）进货环节

进货环节采用了RFID技术，一改往日传统的销售商进货管理，利用读写器获取货物及同时到达的物流信息，对货物自动统计信息并传入信息系统后入库。货物安置在不同的仓库区域后，可以利用固定的电子标签读写器对货物在仓库中的存放状态进行监控，如指定堆放区域、上架时间等信息的统计。当仓储区域货物期限快到时，则自动发出报警信号给中央调度系统通知工作人员。出库时，货物信息的变动同样传送到相应数据库。使用了RFID技术使得货物的登记变得自动化，更加快速准确，减少了人员需求与货物损耗，实现快速提货和取货，并最大限度地减少存储成本。

2）销售环节

商家在销售环节使用电子标签对货物进行统计，只需在主机的系统管理软件上便可查询到货物的详细信息，如存货的种类及数量。同样，在付款台对物品实现自动扫描和计费，取代烦琐的人工收款模式。更令消费者关注的有效期问题，系统对于某些具有实效性商品的有效期限进行监控，提醒商家做出相应的处理，避免过期的损失。同时，商品管理系统对货物进行管理，在缺货时及时通知商家补货，保证货源充足，提高销售环节的效率。

3）运输环节

在货物表面贴上 RFID 标签（如贴在集装箱和外包装上），可以对货物进行跟踪控制。处在运输过程中的货物被安装在车站、码头、机场、高速公路出口等处的读写器读取到电子标签的信息后，连同货物的位置信息传送给货物调度中心的数据库中，准确、及时地更新物流网中的货物信息。

RFID 技术在以上环节中的应用，使得合理的产品库存控制和智能物流技术成为可能。RFID 非常适用于对物流跟踪、运载工具、仓库货架及目标识别等要求非接触采集和交换数据的场合，广泛用于物流管理中的仓库管理、运输管理、物料跟踪和货架识别、商店（尤其是超市）。

3. RFID 技术在超市中的应用

当超市中的商品都贴上 RFID 标签，并配备相应的设备后，就有可能实现自动化、网络化和高效无错的超市管理。超市管理的处理过程如下。

在超市仓库里利用天线接收和传输信息，由信息处理模块与超市管理主机终端相连接，从而实现沟通及处理功能，及时更新仓库信息。在超市销售货架上，固定在货架上的读写器的天线定时地、不间断地向周围的商品发射电磁波，检查商品被取走的情况并报告给超市仓库管理系统。后台管理计算机针对读写器发回的信息，通知仓库及时补充货架上缺少的商品。这样超市管理系统能够随时掌握货物的销售情况，并根据商品的销售状况及时制定销售策略。收银区获取被顾客所挑选的商品的电子标签的信息，记录下消费记录，更新超市管理系统中的信息。为了方便顾客快速查询到商品的产品价格、生产日期、产品产地和保质期等信息，超市可采用移动式的读写器，安装在超市的导购车上，顾客可根据需要查询。

在超市的入口处有采用了 RFID 技术的购物车，在购物车的扶手前端安装了识别电子标签的读写器。顾客只需将商品置于读写器前，屏幕上将显示出该商品的具体价格、名称和产地等。顾客只要在导购车的屏幕上面点击想购买的商品，就能够在屏幕上查询到该商品在超市的具体位置，从而便捷地找到需要的商品。在结账的时候，只要将导购车推过指定的通道，消费总额立即出现在收银台的计算机上。同时，带有标签的货物在通道上被扫描时，会自动反馈给管理系统，更新超市的库存和货架上商品数量等信息。由于商品的数量和价格是随时变动的，超市管理系统应实时更新，保持高度的准确性。超市管理系统自动通过对 RFID 标签信息的读取来完成对店内库存的盘点。

然而，由于 RFID 的标准在全球范围内尚未统一，而商品又要在全球范围内流通，再加上电子标签本身的价格对小商品来说还偏高，因而影响了 RFID 在超市中的全面推广和应用。

无人超市试点已在国内出现，自动解决顾客识别（人脸识别或指纹识别等）、商品识别

和收费等。

14.3.5 射频识别不停车收费系统

使用 RFID 不停车电子收费系统(Electronic Toll Collection,ETC)是世界上最先进的路桥收费方式,通过安装在车辆挡风玻璃后面的电子标签与在收费站 ETC 车道上的微波天线之间的专用短程通信,利用计算机联网技术与银行进行后台结算处理,达到车辆通过收费站不停车就交费的目的,从而加快了路桥收费道口的通行能力。与人工收费通道相比,ETC 车道通行能力可提高 4～6 倍,而且可减少车辆在收费口因交费、找零等动作引起的排队等候,并大大降低了收费口的噪声与废气排放。

对于公路收费系统,由于车辆的大小和形状不同,在电子标签和读写器之间大约需要 4m 的读写距离与快速读写能力,因此系统的频率应该在 UHF 频段,如 902～925MHz。实现方案是将多车道的收费口分成自动收费口和人工收费口两部分。在自动收费车道的道路上方,在距收费口 50～60m 处架设读写器天线,当车辆通过天线下方时,车上的电子标签被天线检测到,读写器判断车辆是否带有有效的电子标签,根据标签是否有效,读写器指示车辆进入不同车道(自动收费口和人工收费口),进入自动收费口的车辆,过路费自动从用户账户上或预付费电子标签上扣除,并用指示灯或蜂鸣器告诉司机收费已完成,不用停车即可通行。人工收费口仍维持现有的操作方式。违规的车辆将被摄像。

RFID 不停车电子收费系统按其功能包括自动识别控制子系统、自动判断子系统、数据采集子系统、车辆检测子系统、闭路电视子系统和信号控制子系统。

(1) 自动识别控制子系统。自动识别控制子系统负责控制收费系统所有设备的运行、收费业务操作的管理,以及与收费站计算机的通信和数据交换,主要由读写器、天线和收费终端等组成。

(2) 自动判断子系统。自动判断子系统主要由光栅、高度检测器和轴数检测器等组成,该系统通过对采集车辆的高度和轴数等参数来判断车型。

(3) 数据采集子系统。数据采集子系统主要由天线和电子标签组成,在电子标签上写有标签编号、车号、车型、车主、应缴金额、余额和有效期等信息,天线读取信息后传送给车道控制机。

(4) 闭路电视子系统。闭路电视子系统主要由车道摄像机和收费站监视器组成,主要用于拍摄违规车辆。

(5) 信号控制子系统。信号控制子系统主要由通行信号灯、偏差信号灯等组成,用于提醒驾驶员正确使用不停车收费车道。

(6) 车辆检测子系统。车辆检测子系统用于激活天线读取电子标签信息,控制通行信号灯、偏差信号灯,并可统计车流量。

14.4 物联网的应用

14.4.1 物联网在物流业中的应用

1. 物流的定义

国家质量技术监督局 2001 年颁布《中华人民共和国国家标准物流术语》,将物流定义

为："物品从供应地向接收地的实体流动过程。根据实际需要，将运输、储存、装卸搬运、包装、流通加工、配送和信息处理等基本功能实施有效地结合。"

上述功能的实现已分散在多个领域，包括制造业、农业、运输业、仓储业、装卸业、物流信息业等，加以整合，就形成复合型的物流服务业。

2. 物流的基本功能

(1) 包装。包装可分为工业包装和商业包装。具体包括生产过程中的半成品和制成品的包装及物流过程中的再包装，它是为了便于物资的运输、保管、装卸而进行的，商业包装则是把商品分装成方便顾客购买和易于消费的小件，或加上生产日期、保质期和提高外观效果。

(2) 装卸搬运。为衔接物资运输、储存、包装、流通加工等作业环节而进行的，伴随着物流的全过程。

(3) 运输。物流组织者将物资从生产地运送到需求地。在不少场合，人们把运输作为物流的代名词。组织者应该选择技术、经济效果最好的运输方式或联运组合，确定运送的交通工具和路线，实现安全、迅速、实时和低成本的效果。

(4) 储存。利用各种仓库、堆场、货棚等，完成物资在从生产到消费整个过程中的保管、养护和堆存等作用，以与最低的成本相一致的最低存货量为顾客服务。

(5) 流通加工。物资流通过程中的辅助加工。为了促进销售、维护产品质量、实现物流和高效率而进行的加工，更有效地满足消费者的需求。

(6) 配送。按用户的订货要求，在物流配送中心完成配货作业后，将配好的物品送交收货人，配送中心一般具备储存功能。配送的实现离不开运输。

(7) 物流信息。包括与上述各种功能实现相关的计划、预测、动态信息、生产信息、市场信息及相关费用等，合理进行信息收集、汇总和统计，以保证物流活动的合理性、可靠性和及时性。现代物流信息以网络和计算机技术为手段。

3. 物流的主要特征

早期的物流概念就是指物资(商品实体)的储存和运输，随着时代的进展，物流管理和物流活动的现代化和集成化不断提高，物流特征概括如下。

(1) 物流的系统化。从系统观点出发，通过物流功能的合理组合，实现物流整体的优化目标。

(2) 物流自动化。物流作业过程的自动化，包括包装、装卸、识别、运输、仓储和流通加工等过程，同时可方便物流信息的实时采集与跟踪，提高物流系统的管理和监控水平。

(3) 物流信息化。现代物流可理解为物资流通与信息流通的结合，早期物流的各个功能之间缺乏有机联系，对物流活动采取事后控制；而现代物流通过实时信息进行控制，提高物流效率，将信息技术、通信技术和网络技术结合应用于物流的各个环节之间，以及物流部门与其他部门之间。

(4) 物流智能化。物流管理由手工作业发展到半自动化、自动化、智能化。自动化过程中包含更多的机械部分，而智能化包含更多的电子化部分，如集成电路、计算机和网络等，在更大范围和更高层次上实现物流管理的自动化，减少人的脑力和体力劳动。

(5) 物流管理专门化。在企业中，物流管理可以作为企业内的专业部门存在，随着企业的发展，企业内的物流部门可能从企业中分离出去成为社会化、专业化的物流企业，并

进一步演变,成立服务专业化的物流企业,即第三方物流企业。

(6) 物流快速实现化。在物流信息系统、作业系统和物流网络支持下,适应用户需求的速度加快,及时配送和迅速调整库存的能力在加强。

(7) 物流标准化。从物流的社会标准来看,可分为企业物流标准、社会物流标准(工业标准、国家标准、国际标准)。从物流的技术标准来看,有物流产品标准、物流技术标准(条码标准、电子数据交换标准)、物流管理标准(ISO 9000、ISO 14000 等)。

4. 智能物流

物联网首先应用于物流行业,是利用信息采集设备、无线射频识别设备、传感器和全球定位系统等与互联网结合起来而形成的网络。

智能物流是指货物从供应者向需求者的智能传送过程,尽量为供方提供最大的利润,为需方提供最好的服务,并尽量消耗最少的自然资源和社会资源,保护好生态环境。

物联网为物流的智能处理提供了多层面的支持,除了利用已有的 ERP 等商业软件进行规划、管理和决策支持以外,还应该为用户提供更多的服务。通过增值性物流服务,拓宽业务范围,增长利润。

物联网将是物流企业间实现协同发展的平台,实现物流、信息流、资金流的三流合一,电子商务、共同配送、全球化生产等先进运营模式,也望逐步实现。

5. 电子商务物流

电子商务(Electronic Commerce, EC)是指通过互联网进行的商务活动,业务范围包括信息的传送和交换、网上订货和交易、网上认证和支付、商品的配送、运输和售后服务及企业间的资源共享等,并利用电子信息技术来降低成本、增加价值和创造商机。

电子商务可使物流实现网络的实时控制。物流的运作以信息为中心,网络传递信息,可实现物流的合理化,协助物流企业对物流的组织和管理,不仅考虑本企业的利益,还要考虑全社会的利益。

电子商务物流的主要特点与前面介绍的基本一致,这也说明了物流业离不开物联网。

14.4.2 物联网在交通管理系统中的应用

先进的地面交通管理系统将信息技术、通信技术、电子传感技术、计算机和网络技术融合在一起,实时、准确、高效、综合地实现交通管理。我国经济的快速发展提高了人们的生活水平,但产生了严重的交通拥堵等问题,为此充分发挥公交调度指挥中心的作用是很重要的,曾采取过一些措施,如在举办国家级、省级的大型活动时采取交通管制等。

基于物联网及其相关技术对公交系统进行设计,达到提高公交系统的自动化管理程度和公交线路的规划水平,提高居民出行的方便性和交通状况改善的目的。

通过对现有公交管理系统进行分析,对公共交通资源数据进行高效管理和维护,为乘客提供车辆快速、实时、定时、安全的运行,解决乘车拥挤和道路拥堵的问题,并对各种车辆提供报警求助、呼叫服务、信息查询、行车路线等。

1）公交管理系统解决方案

采用 RFID 标签、3G 网络、互联网技术，结合 GPS、GIS、视频摄像技术，并以新兴的物联网为背景，提出实现总体解决方案的结构，如图 14.15 所示。

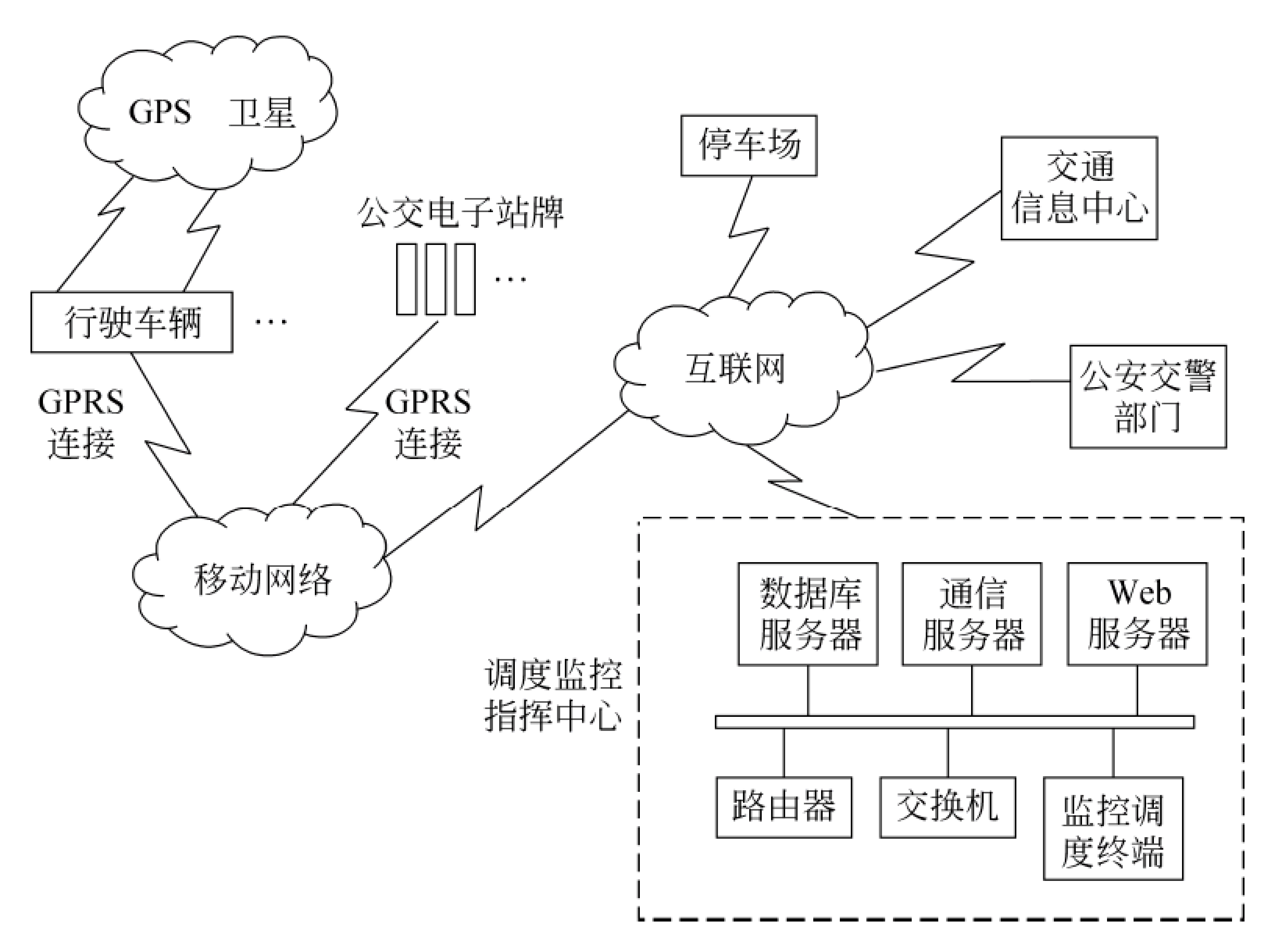


图 14.15　公交管理系统结构

（1）与图 14.15 相关的系统有 GSM（Global System for Mobile communication，全球移动通信系统）、GPRS（General Packet Radio Service，通用无线分组业务，实现基于 GSM 系统的无线分组交换技术）、GIS（Geographic Information System，地理信息系统），是在计算机支持下，对地球表面有关分布数据进行采集、存储、管理、运算、分析、显示和描述的系统。

（2）信息载体。RFID 标签是主要信息载体，分别用于公交站牌、公交车及公交路线上，及时了解公交车的位置。通过温度传感器与 RFID 的结合，乘客可以及时了解车内、外的温度。公交车内部的 RFID 系统主要用于乘客的刷卡消费。

（3）通信网络。可采用 3G 通信网络作为公交车和公交调度中心的通信手段。

2）交通子系统

（1）智能车辆控制系统。通过安装在车辆前部或旁侧的红外探测仪，可正确判断车辆与障碍物之间的距离，遇紧急情况，可发出警报或自动刹车。

（2）交通监控系统。在道路、车辆、驾驶员和交通管理人员之间建立快速联系，通告交通事故、拥堵或通顺的行车路线等。

（3）运营车辆高效管理系统。实现车辆驾驶员与调度管理中心之间的通信，提高商业车辆、公共汽车和出租汽车的运营效率。

（4）交通信息服务。通过装备在道路上、车上、换乘站、停车场上，以及气象传感器、RFID 标签和传输设备向交通信息中心提供实时交通信息，经中心处理后，向需求者提供相关的信息。如果车上装备了自动定位和导航系统，可帮助驾驶员或外出旅行人员选择行驶路线。

（5）交通管理系统。交通管理系统主要提供给交通管理者使用，对道路系统中的交通状况、交通事故和交通环境进行实时监视，并对交通进行实时控制，如信号灯、预防信息、道路管制、事故处理与救援等。

（6）其他。还有停车场管理、货运管理、电子收费系统（ETC）等。

14.4.3 物联网在电网管理系统、智慧城市和智能家居中的应用

1. 电网管理

随着社会经济的发展，用电量不断增加，电网规模不断扩大，影响电力系统运行风险也会增加，因此利用电网设施提高电力供应的安全可靠与质量，控制费用是很重要的。构建以信息化、自动化、互动化为特征的电网，是电力行业的发展方向之一，将物联网的相应技术广泛应用于电力系统的发、输、变、配和用电环节，可带来更大的经济效益和社会效益。

1）物联网在智能化电网中应用的架构

面向智能电网的物联网大致可分为感知层、网络层和应用层3个层次。

（1）感知层。通过传感器、RFID标签等采集信息手段，实现对电网运行的静态或动态信息进行大量采集与分析。对于电网的监控数据基本采用光纤通信方式；对输电线路在线监测、电气设备状态监测，用光纤和无线传感技术传送信息；在用电信息数据采集和智能用电方面，主要涉及窄带、宽带电力线通信、光纤电缆和公用网通信等。

（2）网络层。将从感知层采集来的数据进行转发，通过专用的电力通信网或公用通信网实现，提供了一个高速的双向宽带通信网络平台。

（3）应用层。提供信息处理、计算等的服务设备和资源调用接口，并在此基础上实现各种应用。通过计算、模式识别等技术实现电网相关数据信息的整合、分析处理，进而实现智能化的决策、控制和服务。

2）物联网在智能化电网中应用的设想

（1）电力设备和运行环境的监测。在发电厂内部机组内安置一定数量的传感器测点，可以及时了解机组运行情况，包括各种技术指标和参数。对运行环境监测，如在水电站坝体安装多个传感器，可随时监测坝体的变化情况，以躲避风险，对水位监测与控制，以保证发电和安全。同样，可对风能、太阳能等新电源发电进行在线监测、控制及功率预测等。对输电线路的在线监测也很重要，可提高对输电线路运行状况的感知，包括气象条件，如覆冰、风力、电线振动和偏移、杆塔倾斜程度等。对测到的数据及时传输、联合处理、实时控制，提高电网的技术水平和安全程度。

（2）电力生产管理。管理电力现场作业比较复杂，但很重要。对进入现场的人员进行身份识别和电子工作票管理；对监测到的信息进行分析、过程监控，实现调度指挥中心与现场作业人员的紧密联系，进行日常工作；如果监测到异常信息，则提前做好相应的故障预判，做好设备检修工作，从而提高了自动诊断、设备检修和安全运行水平。

（3）智能用电。实现用户（工业与居民）与电网（厂商）之间的联系，提高供电可靠性、用电效率和节电减排（废气）的功能。

2. 智慧城市

智慧城市可理解为信息化城市，即通过建设宽带多媒体信息网络、地理信息系统等基础设施，整合城市信息资源，建立电子政务、电子商务、劳动社会保险等信息化平台，实现市民经济和社会的信息化。智慧城市的建设应包括以下一些项目。

(1) 公共服务。建设市民呼叫服务中心，实现自动语音、传真、电子邮件和人工服务等多种服务方式，开展生活、生产、政策和法律法规等多方面的咨询和服务工作。

(2) 安居服务。发展社区家居服务、楼宇管理、安全监控和商务办公等。

(3) 教学文化服务。建设教学综合信息网、网络学校、数字化课件、教学资源库、虚拟图书馆、远程教育系统等。

(4) 健康保障体系。健康保障体系包括医疗和福利等。

(5) 交通顺畅和安全。

(6) 文明、平等、公正、廉洁的社会风气，崇高道德和诚信友好的市民作风。

3. 智能家居

家居生活由人力劳动向电器化和智能化方向发展。

智能家居是利用先进的计算机技术，将互联网、移动通信和广播电视与家居生活的各个方面结合在一起，综合实现住宅的智能控制和管理。

智能家居又称智能住宅，实施宅内控制和外界联系。

(1) 宅内控制。宅内控制是指对灯、水、电、气等各个电器进行智能控制，并进行安全监控，同时在适当地方安装监视器，保障人身和财物的安全。

传感器和(或)微处理器使用在家用电器(空调、冰箱、电视机、洗衣机、燃气机等)中，住宅内某些设备的活动和对电器的控制一般利用无线射频技术来实现，这是一种近距离、低功耗、低成本、无须直接连线的技术。

(2) 外界联系。

① 住宅中的计算机、平板电脑、智能手机和(或)电视机通过高速宽带输入，连接互联网进行通信、语音和视频交流、电视和电视剧点播、网上游戏等。

网上银行完成转账和水、电、煤气缴费等功能。

网上购物、外卖订餐、送货到家。

② 网上商务和办公。某些行业可在家进行网上商务联系、举行视频会议。

③ 家庭医疗保健和监护。

④ 网络教育。

习题

1. 你认为居民身份证内应保存哪些数据?
2. 如何保证身份证号的唯一性?
3. 假如身份证最后一位(校验码)不想用罗马数字 X，你认为有其他方法吗?
4. 中国金融集成电路(IC)卡规范与 ISO/IEC 7816 国际标准相比较有哪些关系和特点?
5. 本规范规定的电子存折/电子钱包有哪些功能? 规范中设计的交易流程有什么特点?

6. 论述 MAC 的重要性,如何选择参与 MAC 运算的初始值?假如选择固定值、随机数或操作时间作为初始值,其效果有何差异?
7. 本规范中采用的 3 层密钥管理机制有什么优越性?
8. 借记/贷记 IC 卡进行交易时一般经历哪些步骤?
9. 评价本规范设计的命令系统的优缺点。
10. 什么是真的金融卡和虚拟卡?
11. 移动交付和其他支付方式相比有什么优缺点?
12. 自动化生产流水线涉及哪些设备?
13. 条形码与 RFID 标签在超市中应用所起的作用有什么差别?请叙述它们的优、缺点。
14. 什么是 ETC?请简述其应用场合与特点。
15. RFID 应用和物联网应用有什么主要差别?
16. 物流包括哪些要完成的功能?现代化物流有哪些特征?
17. 现代化物联网与其他网络有什么联系?如何衡量其应用现状和发展前景?

说明:习题中的“本规范”是指中国金融集成电路(IC)卡规范。

附录 A　英文缩写词

ACK	ACKnowledge,确认
ADF	Application Data File,应用数据文件
ADF	Application Dedicated File,应用专用文件
AEF	Application Elementary File,应用基本文件
AES	Advanced Encryption Standard,高级加密标准
AFI	Application Family Identifier,应用系列标识符
AI	Artificial Intelligence,人工智能
AID	Application IDentifier,应用标识符
ANSI	American National Standard Institute,美国国家标准协会
APDU	Application Protocol Data Unit,应用协议数据单元
APf	Anticollision Prefix f,防冲突前缀 f
API	Application Programming Interface,应用编程接口
APn	Anticollision Prefix n,防冲突前缀 n
APP	APPlication,应用程序
ASIC	Application Specific Integrated Circuit,专用集成电路
ASK	Amplitude Shift Key,幅移键控
ATM	Automatic Teller Machine,自动柜员机
ATR	Answer To Reset,复位应答
BCD	Binary-Coded Decimal,二进位码十进制数,二-十进制代码
BER	Basic Encoding Rules,基本编码规则
BGT	Block Guard Time,分组保护时间,块保护时间
BPSK	Binary Phase Shift Keying,二进制相移键控
BSS	Basic Service Set,基本服务集
BWT	Block Waiting Time,分组等待时间
CA	Certification Authority,认证机构
CAD	Card Acceptance Device,卡接收设备,读写器
C-APDU	Command APDU,命令 APDU
CC	Cryptographic Checksum,密码校验和
CD	Coupling Device,耦合设备
CDMA	Code Division Multiple Access,码分多址
CICC	Contactless Integrated Circuit Card,非接触 IC 卡
CID	Card IDentifier,卡标识符

CID	Clock IDentifier,时间标识符
CISC	Complex Instruction Set Computer,复杂指令系统计算机
CLA	CLAss byte,类型字节
CLK	CLocK,时钟
COS	Chip Operating System,片内操作系统
CRC	Cyclic Redundancy Check,循环冗余校验
CPU	Central Processing Unit,中央处理单元
CWT	Character Waiting Time,字符等待时间
D	Data,数据
DAD	Destination node ADdress,目的节点地址
DB	DataBase,数据库
DBP	Differential Bi-Phase,双向差异(编码)
DE	Data Element,数据元
DEA	Data Encryption Algorithm,数据加密算法
DES	Data Encryption Standard,数据加密标准(一种加密/解密算法)
DF	Dedicated File,专用文件
DF	Dual Frequency,双频
DIR	DIRectory,目录
DO	Data Object,数据对象
DPSK	Differential PSK,差分相移键控,相对相移键控
DR	Divisor Receive,接收因子
DS	Divisor Send,发送因子
DS	Digital Signature,数字签名
DSI	Digital Signature Input,数字签名输入
DSSS	Direct Sequence Spread Spectrum,直接序列扩频
EC	Electronic Commerce,电子商务
ED	Electronic Deposit,电子存折
EDC	Error Detection Code,差错检验码
EF	Elementary File,基本文件
EGT	Extra Guard Time,额外保护时间
EIRP	Effective Isotropic Radiated Power,有效的全向辐射功率
EMV	Europay、Mastercard、VISA(与银行卡有关的 3 个组织)
EOF	End Of Frame,帧结束
EP	Electronic Purse,电子钱包
EPC	Electronic Product Code,产品电子代码
EPROM	Erasable Programable Read-Only Memory,可擦除可编程只读存储器
E^2PROM	Electrically-Erasable Programable Read-Only Memory,电可擦除可编程只读存储器

ERP	Enterprise Resource Planning,企业资源计划
ETU(etu)	Elementary Time Unit,基本时间单元
FCI	File Control Information,文件控制信息
FCP	File Control Parameter,文件控制参数
FDMA	Frequency-Division Multiple Access,频分多路访问
FDX	Full DupleX,全双工
FDT	Frame Delay Time,帧延迟时间
FHSS	Frequency Hopping Spread Spectrum,跳频扩频
FIFO	First In-First Out,先进先出
FM	Frequency Modulation,调频制
FMD	File Management Data,文件管理数据
FSK	Frequency Shift Keying,频移键控
FTC	Financial Transaction Card,金融交易卡、金融卡
FTDMA	Frequency and Time Division Multiple Access,频分和时分多路访问
FTP	File Transfer Protocal,文件传输协议
FWT	Frame Waiting Time,帧等待时间
FZ	Fabrication Zone,制造代号区
GIS	Geographic Information System,地理信息系统
GPRS	General Packet Radio Service,通用无线分组业务
GPS	Global Positioning System,全球定位系统
GPU	Graphic Processing Unit,图形处理器
GSM	Global System for Mobile communication,全球移动通信系统
HDX	Half DupleX,半双工
HF	High Frequency,高频
IaaS	Infrastructure as a Service,基础设施即服务
I-block	Information block,信息分组、信息块
IC	Integrated Circuit,集成电路
ICC	Integrated Circuit Card、IC Card,集成电路卡
ID	IDentifier,标识符
IDO	Interindustry Data Object,行业间数据对象
IEC	International Electrotechnical Commission,国际电工委员会
IEEE	Institute of Electrical and Electronics Engineers,电子电气工程师协会
IFD	InterFace Device,接口设备、读写器
IFS	Information Field Size,信息字段大小(长度)
IFSC	Information Field Size for the Card,卡的信息字段长度
IFSD	Information Field Size for the interface Device,接口设备的信息字段长度

IIN	Issuer Identification Number,发行者标识号
IMSI	International Mobile Subscriber Identity,国际移动用户识别码
INF	INformation Field,信息字段
INS	INStruction byte,指令字节
I/O	Input/Output,输入/输出
IPTV	Internet Protocol Television,互联网协议电视,网络电视
IRQ	Interrupt ReQuest,中断请求
ISBN	International Standard Book Number,国际标准书号
ISM	Industrial、Scientific、Medical,工业、科学、医疗
ISO	International Standard Organization,国际标准化组织
IT	Information Technology,信息技术
ITU	International Telecommunication Union,国际电信联盟
IZ	Issuer Zone,发行代码区
KM	Master Key,主密钥
KS	Session Key,过程密钥、会晤密钥
L	Length,长度
LAN	Local Area Network,局域网
LCS	Life Cycle Status,生命周期状态
LEN	LENgth,长度
LF	Low Frequency,低频
LRC	Longitudinal Redundancy Check,纵向冗余校验
LSB	Least Significant Bit,最低有效位
LTE	Long Time Evelution,长期演进
MAC	Message Authentication Code,报文鉴别码
MCU	MicroController Unit,微控制器
MES	Manufacturing Execution System,制造执行系统
MES	Management Execution System,管理执行系统
MF	Master File,主文件
MF	Medium Frequency,中频
MFM	Modified Frequency Modulation,改进调频制
MSB	Most Significant Bit,最高有效位
MW	MicroWave,微波
N/A	Not Applicable,不能用
NAD	Node ADdress,节点地址
NFC	Near Field Communication,近距离通信
NRZ	Non Return to Zero,非归零制
NVM	Non-Volatile Memory,非易失性存储器

O2O	Online to Offline,线上到线下
OEM	Original Equipment Manufacture,原始设备制造
OOK	On-Off Keying,开关键控
P1-P2	Parameter byte,参数字节
PaaS	Platform as a Service,平台即服务
PAN	Primary Account Number,主账号
PBOC	the People's Bank Of China,中国人民银行
PCB	Protocol Control Byte,协议控制字节
PCD	Proximity CD,接近式耦合设备
PCOS	Payment COS,支付 COS (参见 COS)
PDM	Pulse Duration Modulation,脉冲宽度调制
PFM	Pulse Frequency Modulation,脉冲频率调制
PICC	Proximity ICC,接近式 IC 卡
PIE	Pulse Interval Encoding,脉冲间隔编码
PIN	Personal Identification Number,个人标识码
PIX	Proprietary application Identifier eXtension,专有的应用标识扩展
PK	Public Key,公共密钥
POS	Point Of Sales,销售点
PPM	Part Per Million,百万分之几
PPM	Pulse Position Modulation,脉冲位置调制
PPS	Protocal and Parameters Selection,协议参数选择
PSK	Phase Shift Keying,相移键控
PUK	PIN Unblocking Key,PIN 解锁密码
PUPI	Pseudo-Unique PICC Identifier,伪唯一 PICC 标识符
RAM	Random Access Memory,随机存储器
R-APDU	Response APDU,响应 APDU
R-block	Receive-block,接收分组、接收块
REQA	REQuest Command (Type A),请求命令(类型 A)
REQB	REQuest Command (Type B),请求命令(类型 B)
RF	Radio Frequency,射频
RFID	Radio Frequency IDentification,射频标识
RFU	Reserved for Future Used,保留于将来使用
RISC	Reduced Instruction Set Computer,精简指令系统计算机
ROM	Read-Only Memory,只读存储器
RSA	Rivest、Shamir、Adleman(三人名),(一种非对称加密/解密算法)
RST	ReSeT,复位、总清
R/W	Read/Write,读/写

SaaS	Software as a Service,软件即服务
SAD	Source node ADdress,源节点地址
SAM	Secure Access Module,安全存取模块
SAW	Surface Acoustic Wave,表面声波
S-block	Supervisory block,管理分组、管理块
SC	Security Code,安全代码
SC	Smart Card,智能卡
SDMA	Space Division Multiple Access,空分多址
SE	Secure Element,安全元件
SE	Security Environment,安全环境
SFI	Short File Identifier,短文件标识符
SHF	Super High Frequency,特高频
SIM	Subscriber Identity Module,用户识别模块
SM	Secure Messaging,安全报文
SoC	System on Chip,片上系统
SOF	Start Of Frame,帧开始
SUID	Sub Unique IDentifier,子唯一标识符
SW1-SW2	状态字节
TAC	Transaction Authorization Cryptogram,交易验证码
TCP/IP	Transmisson Control Protocol/Internet Protocol,传输控制协议/互联网协议
TDMA	Time Division Multiple Access,时分多路
TLV	Tag、Length、Value,标志、长度、值
TV	Television,电视机
UHF	Ultra High Frequency,超高频
UID	Unique IDentifier,唯一标识符
USB	Universal Serial Bus,通用串行总线
VCD	Vicinity CD,邻近式耦合设备
VICC	Vicinity ICC,邻近式集成电路卡
WDC	World Data Center,世界数据中心
WLAN	Wireless Local Area Network,无线局域网
WWAN	Wireless Wide Area Network,无线广域网
XOR	logical eXclusive-OR operation,异或逻辑操作

参考文献

[1] International Standard ISO 7810. Identification Cards. Physical Characteristics，2003.

[2] International Standard ISO 7811. Identification Cards. Recording Technique，2001-2004.

[3] International Standard ISO/IEC 7816. Identification Cards. Integrated Circuit(s) Cards，Part1-Part13，Part15.

[4] International Standard ISO/IEC 14443. Identification Cards. Contactless Integrated Circuit(s) Cards-Proximity Cards，Part1-Part4.

[5] International Standard ISO/IEC 15693. Identification Cards. Contactless Integrated Circuit(s) Cards-Vicinity Cards，Part1-Part3.

[6] International Standard ISO/IEC 18000. Information Technology-Radio Frequency Identification for Item Management，Part1-Part4，Part6/7.

[7] 王爱英.智能卡技术——IC卡、RFID标签与物联网[M]. 4版. 北京：清华大学出版社，2015.

[8] 陆永宁.非接触IC卡原理与应用[M].北京：电子工业出版社，2006.

[9] 周晓光，王晓华.射频识别(RFID)技术原理与应用实例[M].北京：人民邮电出版社，2006.

[10] 游战清.无线射频识别(RFID)与条码技术[M]. 北京：机械工业出版社，2007.

[11] 郎为民.射频识别(RFID)技术原理与应用[M]. 北京：机械工业出版社，2006.

[12] 中国人民银行.中华人民共和国金融行业标准——中国金融集成电路(IC)卡规范[S]，2005.

[13] 赵健，肖云，王瑞. 物联网概述[M].北京：清华大学出版社，2013.

[14] 刘丽军，邓子云. 物联网技术与应用[M]. 北京：清华大学出版社，2012.

[15] 金光，江先亮. 无线网络技术教程[M]. 北京：清华大学出版社，2011.

[16] 胡道元，计算机局域网[M].4版. 北京：清华大学出版社，2010.

[17] 王爱英. 计算机组成与结构[M].5版. 北京：清华大学出版社，2013.

[18] 陈艳.基于RFID的井下人员跟踪管理系统的研究[J]. 金卡工程，2008(4).

[19] 辛国斌，田世宏. 国家智能制造标准体系建设指南(2015年版)[M]. 北京：电子工业出版社，2016.

[20] 邱建华，冯敏. 生物特征识别[M]. 北京：清华大学出版社，2016.

[21] 张尤腊，周锡令，董士海. 微信使用教材[M]. 深圳市软件行业协会出版，2017.